Security Vulnerabilities of Cryptocurrency Wallets -A Systematic Review

*[1]Abdulkadir R. Kirobo
[1]Department of Information Communication Technology, Arusha Technical College, Arusha, Tanzania
abdulkadir.kirobo@atc.ac.tz | akirobo@yahoo.com

Received: 01-AUG-2024; Reviewed: 01-OCT-2024; Accepted: 15-NOV-2024
https://dx.doi.org/10.4314/fuoyejet.v9i4.4

REVIEW PAPER

Abstract— The cryptocurrency wallet security has been among the hot issues concerning its adoption. It hinders most users and government from adopting crypto-market. There are several security issues reported by the study such as scams, hacks, and theft in digital coins particularly cryptocurrency. This study has deployed literature review techniques to bring awareness on the frequently used vulnerabilities and to suggest the way to mitigate and prevent such vulnerabilities. Numerous methodologies suggested by prior-literatures has been used to mitigate, detect, and prevent any security threats towards crypto-wallet. The study has found that the cryptocurrency wallet is subjected to several attacks which are born by the general internet protocols loopholes, those attacks born by the presence of security vulnerabilities awareness, and those attacks resulted from the nature of blockchain systems. Several users have been victimized by the scammers, hackers, and fake investment schemes due to lack of knowledge base concerning security vulnerabilities. This study recommends the usage of several security policies to combat those vulnerabilities which include usage of Insurance policies, Security scans policies, and deployment of AI systems to mitigate any security vulnerabilities.

Keywords— Cryptocurrency Wallet, Security Vulnerabilities, Double Spending, Detection and Prevention Techniques..

1 INTRODUCTION

This security issues have been the main concerns in all networked computers. The users are needed to lock all doors and windows to secure the system against any security vulnerabilities meanwhile the attackers are always looking for one loop hole to attack. Several attacks have been reported recently in various professional fields such as healthcare systems (Silvestri, 2023), Internet of Things (IoT) (Lone, Mustajab, & Alam, 2023, Ahmad, et al, 2019), cloud computing (Alam, Shahid & Mustajab, 2024), social media (Parthiban, Rajeswari, Ravichandran, 2024 and Raheed, et al, 2024), e-commerce (Albshaier, Almarri, Hafizur 2024), big data (Darwish, 2024 and Alhazmi, 2022), blockchain technology (Albshaier, Almarri, Hafizur 2024), and in cryptocurrency (Rai, Dubey, 2024). The attackers are taking advantages of security loop holes/vulnerabilities that may arise from time to time. The internet defense mechanism has been detecting new security vulnerabilities known as Common Cybersecurity Vulnerabilities (CVE) everyday (Mitre, 2024). According to SecurityScorecard (2024) there was increase in CVE by more than 4000 issues from 48,196-CVE in December 2022 to 52286-CVE in December 2023. Attackers are deploying these CVE to scams potential victims, for example in 2020 they have scammed crypto-markets customers and earned millions of U.S Dollars (Bartoletti et al, 2021). The purpose of this study is to explore the security issues concerned in cryptocurrency wallets that might be used by the fraudsters to scam the crypto-market.

*Corresponding Author: abdulkadir.kirobo@atc.ac.tz

Section B- ELECTRICAL/COMPUTER ENGINEERING & RELATED SCIENCES
Can be cited as:
Kirobo A.R. (2024). Security Vulnerabilities of Cryptocurrency Wallets -A Systematic Review. FUOYE Journal of Engineering and Technology (FUOYE**JET), 9(4), 580-590.** https://dx.doi.org/10.4314/fuoyejet.v9i4.4

The network usage stakeholders are required to be aware of these security vulnerabilities so as to bridge the gap between the attackers and security counter measures. This study has researched all possible cryptocurrency wallet`s security vulnerabilities so as to bring awareness to stakeholders in order to minimize its impacts.

Most victims of cybersecurity are aware of the presence of such vulnerability but they fail to take adequate precautions (Bartoletti et al, 2021). This is because they have been assuming that all doors are closed for any security threats but they end up being scammed. This study is helpful as it covers the content using latest literature of which the latest vulnerabilities has been cited in those literature and hence it includes wide range of security vulnerabilities that has ever been covered by any single article. The study has explored types of cryptocurrency wallet`s attacks and their respective counter measures to prevent such attacks.

The rest of this study is distributed as follows, Section-2, describes the methodology used to select the literature to be used in this study, Section-3 outlines the background of cryptocurrency vulnerabilities that deemed necessary to cover all related security concerns in cryptocurrency wallet, Section-4 discuss the findings and suggest the best approach to be deployed in order to prevent any vulnerabilities found in cryptocurrency wallet, and finally the conclusion and recommendation are provided in section 5 of this manuscript.

2. LITERATURE REVIEW

This study explores the latest security vulnerabilities on cryptocurrency wallets. Numerous sources were used to extract information concerning the wallet security. These literatures have been used to answer two research questions as follows: Question-1: What are the categories of security vulnerabilities for wallet of cryptocurrency?

Question-2: How to prevent those security vulnerabilities against crypto-wallet scams and hackers?

The study has adopted the systematic literature review which has been published within 6 years from 2018 to 2024. Those publication years were selected because currently emerged security issues and vulnerabilities are the ones used by the scammers and attackers. Those contents found in the sources published before 2018 were thoroughly searched in all sources for replacement above 2017. Apart from contents reported from literatures, other sources such as security vulnerability databases were scrutinized to make sure the search results have covered any recently reported security incidents. The search procedure was performed in three steps:

Step-1: The search was performed using keywords found in the abstracts of a particular study.

Step-2: The abstract of those articles was thoroughly read to find out if it covers a lot concerning the wallet security.

Step-3: Those passed articles were downloaded and the researchers have read the full articles from abstract to references.

2.1 SEARCH RESULTS FROM DATA SOURCES.

The online data sources deployed in this study comprises of IEEE Xplore, ACM Digital Library, Springer Link library, Elsevier, and Google Schoolar. The table-1: below shows the summary of the search results articles used in this study. Several combinations of keywords were used for searching purpose from all sources. Google scholar was used as pilot search engine because all other sources can easily pop-ups in google scholar. This was followed by IEEE Xplore and Springer Library because most books concerning special security issues were easily found in those sources. In case the combinations resulted in no matched article or the search resulted found too old publications (before 2018) the search expanded to ACM and Elsevier libraries. The search procedures were divided into four categories: Cat1 (Google Schoolar), Cat2 (IEEE Xplore), Cat3 (Springer), Cat4 (ACM and Elsevier). The keywords used are divided into three subcategories namely:

Categ1: Cryptocurrency security vulnerabilities, security threats, Crypto-wallet security, double spending vulnerability, cybersecurity, and cryptocurrency wallets.

Categ2: Internet scams, cryptocurrency attack, cybercrime attack.

Categ3: Defense mechanism against cybercrime, cybersecurity detection and prevention, security challenges, cybercrime, and cryptocurrency attack.

All graphics will appear in print as black and white, but coloured equivalent might appear in online version. Ensure all graphics will shows correctly when printed in grayscale.

Table-1: Total Publications

SN	Category	Keywords	Google Scholar	IEEE Xplore	Springer	ACM	Elsevier	Total
1	Categ1	Cryptocurrency security vulnerabilities, security threats, Crypto-wallet security, double spending vulnerability, cybersecurity, and cryptocurrency wallets.	128	29	133	310	36	1036
2	Categ2	Internet scams, cryptocurrency attack, cybercrime attack	337	2	67	128	55	589
3	Categ3	Defense mechanism against cybercrime, cybersecurity detection and prevention, security challenges, cybercrime, and cryptocurrency attack.	283	5	94	295	31	708
Total			748	36	294	733	122	2333

2.2 SEARCH RESULTS AND FILTERING TECHNIQUES

The filtering techniques applied in three steps to remove some articles from this study as follows:

Step-1: The search was performed using keywords found in the abstracts of a particular study. In this category the study has found 2333 articles. In this step, there are some articles from google scholar were not published from peer reviewed journal were instantly discarded.

Table-2: Filtered Publications by Abstract Reading

SN	Category	Google Schoolar	IEEE Xplore (Open Access	Springer	ACM	Elsevier	Total
1	Categ1	52	12	58	83	17	222
2	Categ2	61	2	42	8	23	136
3	Categ3	38	3	33	1	18	93
Total		151	17	133	92	58	451

Step-2: The abstract of those articles was thoroughly read to find out if it covers a lot concerning the wallet security. these filtering techniques help us minimize the study sources to 451 articles which was further searched in step-3 below. The results are shown in the table-2 above .

Step-3: Those 451 articles found in step-2 were

http://.doi.org/10.46792/fuoyejet.v9i4.4 engineering.fuoye.edu.ng/journal

downloaded and the researchers have read the full articles from abstract to references. Some recently published articles were removed from this study because it refers way too old publications on their references. Others were filtered out due to having little coverage concerning the latest security and end up with 78 articles as shown in table-3 below.

Table-3: Filtering and Removing Techniques: Full Text Reads

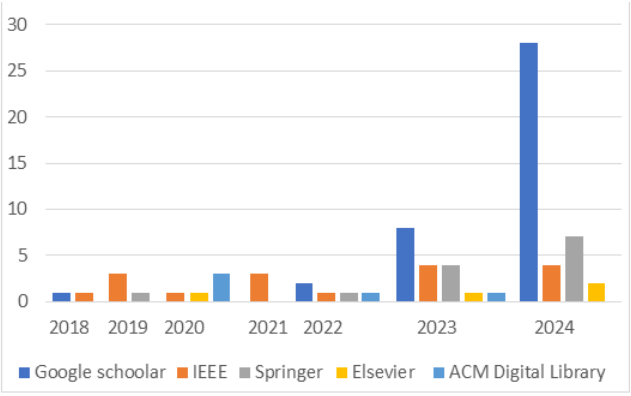
SN	Category	Google Schoolar	IEEE	Springer	ACM	Elsevier	Total
1	Categ1	12	12	5	3	2	34
2	Categ2	15	2	5	1	1	24
3	Categ3	12	3	3	1	1	20
Total		39	17	13	5	4	78

The 78 articles which has passed for contribution in this study has been summarized as shown in table-4 below.

SN	Sources	Total Articles	2018	2019	2020	2021	2022	2023	2024
1	Google Schoolar	39	1				2	8	28
2	IEEE Xplore	17	1	3	1	3	1	4	4
3	Springer	13		1			1	4	7
4	Elsevier	4			1			1	2
5	ACM Digital Library	5			3		1	1	5
Total Articles		78	2	4	5	3	5	18	41

The figure-1 below shows the summary of number of articles against year of publications

Figure-1: Number of Publications Per Year



3. Background Of Cryptocurrency Vulnerabilities

Blockchain based cryptocurrency is composed of public keys and private keys. These keys are kept on cryptocurrency-wallet, unlike traditional wallets which keep real money, the crypto-wallet only stores the cryptographic records about the money instead of real currency values. There are two types of wallets which ranges from software/digital and hardware wallets (Suratkar et al, 2020). Digital wallets are further divided into online wallet (Ye, 2023) desktop wallet Popchev et all, 2023), and mobile wallet (Mirza, & Rahulamathvan, 2023). Meanwhile the hardware wallet is sub-divided into two types, printed paper wallet and USB-storage based wallet (Sharad & Chavan, 2024). The printed paper wallet is the most secured wallet but if source is compromised there is no way to access the crypto asset (Dwivedi et al, 2023). The other wallets are susceptible to several kinds of online security risk such as identity theft (Anitha et al, 2024), Ransomware (Emary and Yagi, 2024), phishing (Angafor et al, 2024), deanonymization (Houy et al, 2023), denial of service and channel amplification attack (Kish et al, 2024), long-range attacks, mining malware, and SIM swapping (Rao, & Suvarna, 2023), SQL injection (Sommervoll et al, 2024) and other cybercrime. In addition, crypto-wallets are also vulnerable due to the nature of blockchain technologies transactions. These hacking activities including Defi hacks (Carlisle, 2023), SLAM attack (Bleeping, 2024), double-spending attack (Lokendra et al, 2024), majority attack (Gans & Halaburda, 2024), eclipse attack (Baninemeh et al, 2024), sybil attack (Xie & Yan, 2024), BGP hijacking attack (Li et al, 2024), Liveness attack and Balance attack (Xu et al, 2024). Furthermore, there are other scams that target crypto-wallet such as adversarial attacks (Ryu, & Choi, 2024) Ponzi schemes, fake crypto market, cross-site scripting, and cross-site request forgery (Shukla et al, 2023). These attacks take the advantages of some blockchain network structure and transactions protocols. Each cyber security issues uses specific security loopholes to under goes such attack, the details are discussed below.

3.1 Identity Theft

Identity theft is a criminal activity of which the personal financial information is stolen by another person to commit fraud or making unauthorized financial transactions. Users are redirected to malicious website that poses serious threats once accessed. These websites contain various forms of viruses such as Nimda, Morris Worm, ILOVEYOU, tuxnet, SQL, conficker, crypto-locker, slammer, trojan virus, tinba, adware, and spyware which can infect the victims' devices. Users tend to fall into these traps and loses monetary resources or potential personal monetary details like PAN, Aadhar, and Credit Cards (Alghamdi, & Nor, 2024). Sometimes personal identity is compromised through fake cryptocurrency exchange markets of which the websites comprise of all exchange futures necessary for daily transactions from one crypto-currency to another. Several other types of attack can be accomplished after comprising the victim's identity.

Identity theft has become prevalent cybercrime, and network users need to take preventative measures to minimize its impact. Some literatures have suggested deploying blockchain technology to minimize the

http://.doi.org/10.46792/fuoyejet.v9i4.4 engineering.fuoye.edu.ng/journal

impacts of identity theft by storing information in several distributed servers (Pathare et al, 2022). The Cryptocurrency wallets should be distributed in small wallets of very low values to avoid major loss once victimized. Identity theft that are resulted from phishing attacks it can be prevented by avoiding anything that could lead to phishing attacks.

3.2 Ransomware

Ransomware is a system designed to disable the data access of the victim's computer. There are several families of ransomware such as Cerber, Locky and CryptoWall (O'Kane et al, 2018). The attackers are taking advantage of having accessible internet, infection mechanism, encryption options, abundant storage, and cryptocurrency payment systems. Attackers are normally avoiding detections by forcing their victim to pay through cryptocurrency (Obi et al, 2024).

Ransomware can be prevented by avoiding all network vulnerabilities that could be used by the attackers. This include the blockchain based distributed storage of which the data are distributed to multiple data storage servers that share the load to enhance data security and storage efficiency (Silvestri, 2023). This would swat away any ransomware attacks as there is no data would be compromised due to lack of access from single device as the blockchain networked computers are accessible from all devices. It can also be prevented by taking several precautions such as regular data backup, report it, consult your antivirus provider, don't take anything for granted, not install unknown software, and do not pay out any money to anyone (Vistro et al, 2024).

3.3 Phishing

Attackers have been using phishing attempts to trick their victim to entails into giving the attacker private and sensitive information about them. They may disguise themselves as legitimate representative of a certain company that offers oneself to help you on your financial activities (Navaneethakrishnan et al, 2023). They sometimes pose as legitimate websites offers a certain service in order to acquire and stole users' information. Also, criminals have been phishing by using malicious ads on targeted trusted sites to spreads the ransomware (Vistro et al, 2024). In addition to that phishers create a new website by imitating the original websites that stole users' information for their own usage (Navaneethakrishnan et al, 2023).

Most phishing victims are targeted through websites, which comprises of fake websites, malicious ads, and imitated websites which traps its users towards compromising their information. There are several methods used to detect phishing websites such as usage of deep learning empowered phishing URL detection (Subashini, & Narmatha, 2024), faster recurrent convolutional neural network (Nanda & Goel, 2024), long-term memory, support vector machine, and random forest (Tapsoba et al, 2024). The challenges of these methods are that the attackers are constantly changing the way to avoid these detections mechanisms, and therefore some precautions must be adhered by users well in advance before being victimized by scammers. Avoid phishing by taking precaution against spam, avoid using unsecured networks, avoid unknown mail attachment, and educate the officials to bring awareness on phishing activities (Angafor et al, 2024).

3.4 Deanonymization Attack

De-anonymization or deanonymization is a strategy of cross-referencing anonymous data with other data-sources to re-identify the original data-source (Houy et al, 2023). Cryptocurrency wallet has been anonymous in that the wallet owner is kept secret during transactions. The private and public keys are utilized to authorize transactions but not user`s identity. This feature has been useful to protect customers from potential scammers. Deanonymization attacks has been performed to identify the crypto-wallet owners. The deanonymization`s ultimate goal is to retrieve the possible relationships between any cryptocurrency transactions (or addresses) and physical IP-Addresses (Biryukov & Tikhomirov, 2019). Once the relationship is successfully matched, the attackers could use such information to scam the victims.

In order to minimize this attack, the wallet owners are encouraged on the usage of different addresses on every coin storage (Kumar et al, 2023). Another alternative to mitigate deanonymization is to deploy new crypto-techniques of which the address of each coin storage is generated automatically by the blockchain systems. This would help users from headache of usage of new address every time they want to store a coin. Normally IP addresses are not linked to personal identity but it could be used to locate the device and hence identify the registration details from Internet Service Provider (ISP).

3.5 Denial of Service Attacks and Channel Amplification Attacks

Denial of Service (DoS) attacks have emerged to be the threats in cryptocurrency exchanges platforms. Blockchain systems are also vulnerable to the distributed denial of services (DDoS) attack. Unlike DoS which comprises of sending many requests from the same source, DDoS attacks deploys methodologies of which many requests are sent from several sources to make the victims web services not reachable by the reliable customers (Abhishta et al 2019). During such period the attackers uses those opportunities by performing fake exchange activities on the crypto-exchange platforms without any validations from the real vendors (Achary et al, 2023). Normally most DoS attackers deploys channel amplification attacks techniques to boost the number of request sent from specific channels.

The Blockchain based exchange platforms act as third-party which brings together the crypto-coins buyers and sellers from different cryptocurrencies. Deep learning techniques has been suggested for potential DoS attack detection before it effect the whole platform. This can be performed by evaluating experimental real request outcomes from networks level data acquisition and service level DDoS attacks in the Bitcoin system (Achary et al, 2023). This deep learning techniques act as defense mechanism beyond blockchain systems.

http://.doi.org/10.46792/fuoyejet.v9i4.4 engineering.fuoye.edu.ng/journal

3.6 Long-Range Attack

Due to the presence of Proof-of-Stake (PoS) protocols in blockchain systems it creates a loop-holes on the limitations of the size of blockchain (Deirmentzoglou et al, 2019). Long-range attackers re-fabricate fake blocks of transactions to overpower the original chains (Sarah et al, 2020). There are several strategies reported by the researchers to counter these attacks by strategically deploying Proof-of-Work (PoW) protocols into Proof-of-Stake (PoS) in the same blockchain systems (Sarah et al, 2020). This would prevent any re-construction of malicious chain.

3.7 Mining Malware

In this attacking techniques the scammers use the malware to re-direct the incentive transactions sent to the victim's wallet.In a traditional malware such as ransomware, it deploys similar approach of hijacking the systems but instead of acquiring large amount of money at once the mining malware collects small amounts in a particular period of time without being detected. These attackers use phishing, and malicious websites to lure their victims (Sayeed & Marco-Gisbert, 2018). It can be avoided by following several strategies deployed in phishing such as taking precautions against spam, avoid using unsecured networks, and avoid unknown mail attachment.

3.8 SIM Swapping

The access to the cryptocurrency wallet is mainly secured by using two factor authentications which comprises of strong password and mobile phones verification codes. The codes are normally sent to the customers registered mobile phones to verify any login attempt. The attackers hijacking the mobile phones of a victims to acquire full access of the desired account to exploit the accessible mobile service for perpetration purposes (Kim et al, 2022). Due to the presence of vulnerabilities in two factor authentication systems, there must be some mobile applications that can be used to communicate with the personal devices instead of sending real SMS to avoid SIM swapping (Jover, 2020).

3.9 SQL Injection

Structured Query Language (SQL) injections is a technique used by the attackers to acquire the access of unauthorized information from the websites such as passwords, credit card details, and Personal user information (Herskind et al, 2020). These attacks may lead to DoS attacks and eventually the victims could be losing huge amount of crypto-currency. SQL injection can be detected and prevented by using machine learning techniques (Khare & Badholia, 2023).

3.10 DeFi Hacks

DeFi stands for Decentralized Finance, is a type of financial systems introduced by the blockchain systems using cryptocurrency of which no third party is required to authorize and validate DeFi services transactions. The DeFi services such as money lending, borrowing, and securities are offered automatically by using blockchain smart contracts which authorize the services. The hackers are utilizing this fully autonomous environment to steal the money from mostly crypto-finance companies which offers decentralized monetary lending services by deploying smart contracts (Li et al, 2022). The attackers are posing themselves as legitimate customers acquiring loan services in a crypto market and receive the loan which would never be recovered. Due to DeFi hacks the crypto-market has suffered a total loss of about 3.24 billion USD in four years from April 30-2018 to April 30-2022 (Zhou et al, 2023). There are several tools used for detection and prevention of DeFi attacks such as smart contracts fuzzing, static analysis, symbolic execution, and formal verification (Zhou et al, 2023).

3.11 SLAM Attack

SLAM stands for Spectra based Linear Address Masking (SLAM). This attack capitalized on the vulnerabilities similar to the addressing mechanism of the Intel-Central Processing Unit (CPU). The attackers can have access of very sensitive data through SLAM attacks such as root password of a device which may lead to further losses. Once the login information is compromised everything in the computer are vulnerable which may include any financial information such as banks cards, crypto-wallet credentials, and other webpage login details.

3.12 Double-Spending Attack

Double spending attack is the attack directly related to the crypto-wallet protocols of which the consensus mechanism is based on the smart contracts. The coins are validated by the nearby servers before being spent or transacted to another account. This checking mechanism is slow process that gives opportunity for attackers to reconstruct the chain that would represent the same coins which were in the verification process in the decentralized systems. The attackers are capable of deploying sybil attacks to further increase the propagation delay for the legitimate customers so as to win the mining race (Tyagi, 2024). Double spending preventions can be carried out by introducing centralized validation and authorization systems that would double check the coins before executions. Sometimes sybil attacks is used to facilitate double spending activities thus by preventing this attack would automatically reduce the chance of these hackers to succeed.

3.13 Majority Attack

The majority attack is achieved by the computing powers of certain group in the decentralized distributed ledger of which the proofs-of-works and smart contracts validations are conducted based on majority node`s votes (Gans & Halaburda, 2024). This attack is also known as 51% attack or >50% attacks of which the attackers have more computing power exceeding 50% of the mining powers in the crypto-market. The purpose of this attack is to commit double spending attack. The crypto-market are susceptibility to these attacks when corrupt version of the chain is introduced into the systems and totally isolated from real version to avoid detections (Sayeed & Marco-Gisbert, 2018). The deployment of Blockchain systems and Artificial intelligence in the crypto-market is regarded as the best ways to keep yourself safe from these attackers (Sayeed

http://.doi.org/10.46792/fuoyejet.v9i4.4 engineering.fuoye.edu.ng/journal

et al, 2019). Artificial intelligence would act as a defense mechanism that detect any potential threats while proof-of-works and proof of stakes act as consensus mechanism that can be useful to approve transactions.

3.14 Eclipse Attack

Eclipse attack is performed by isolating the victims from the rest of the network to avoid detection and accomplish double spending attacks (Sekiguchi & Tanaka. 2024). An eclipse attacker involves isolating a specific node within the network by redirects the target's incoming communications and outgoing connections away from neighboring nodes to other nodes that under the hacker's control. In this process the attackers increase the chance of having more time to negotiate double spending by manipulating the request sent to the victims and generating new fake responses from their own corrupted nodes to represent the legitimate request. Unlike majority attack which involves creations of several fake nodes or IP addresses to outnumber the legitimate nodes to have computing power which most of the time seems difficulty, eclipse attack would use few nodes and freezing the victim's node to perform double spending attack.

3.15 Sybil Attack

The Sybil attack deploys similar techniques as that of 51% attack. In a Sybil attack, the hackers develop a large number of fake nodes in the network to acquire computing power (Sayeed et al, 2019). The attackers use several devices such as virtual machines, and Internet Protocol (IP) addresses to pose as a large collection of nodes that have a huge say on smart contracts. Unlike 51% attack which require physically more power than the crypto market which economically impossible, sybil attack would deploy fake nodes generation techniques to create more computing power than the market. The sybil attack, eclipse attack, and majority attack can be prevented by adopting mitigation techniques that can produce immunity to the hackers. These includes deploying a penalty system for delayed block submission, delayed Proof of Work (dPoW), utilizing PirlGuard Protocols, exercising Chain-Locks, and introducing Merged Mining Techniques (Sayeed et al, 2019).

3.16 BGP Hijacking Attack

Border Gateway Protocol (BGP) is a network protocol used by ISP specifically designed to route the traffic for the network packets to the desired network. BGP hijacking or routing attack is a network hijacking technique of which the internet routing is diverted for the benefits of the attackers (Sekiguchi & Tanaka, 2024). BGP exploits can be prevented by adopting recognized network routing tables and compare with fake route announcement, delayed BGP adoptions for 24 hours, listen and whisper techniques, and deploying improved BGP protocols (Morris et al, 2024).

3.17 Balance Attack

The Balance attack is the attack intended to gain the majority of the mining power by enforcing the delay on the subgroup of legitimate nodes (Li et al, 2020). This techniques is similar to eclipse attack which hide a certain node to communicate to other node, in balance attack several nodes are kind of hidden for a particular period of time by delaying its communications to other nodes (Pavithran et al, 2021). The balance attacks aims to exploit the ghost-protocol by separating the blockchain branch from the other nodes in the network (Li et al, 2020). The balance attack can be prevented by deploying cyberbiophysical in the network systems which comprises of sensing, data processing, control, and networking (Shankar et al, 2023).

3.18 Liveness Attack

Liveness attack involves the delaying of confirmation time of targeted cryptocurrency transactions (Pavithran et al, 2021). It is achieved in three phases namely attack preparation phase, transaction denial phase, and blockchain retarder phase (Li et al, 2020). In this scenario the attacker will hold back any transactions from certain nodes until they have successfully built a longer block than public block. In this case the hackers would have commit double spending attack on the blockchain systems. Liveness attack can be prevented by shortening the time to taken to accept the blocks, introducing new procedure to slash mis-behaving block validators, and increase the stake needed to became legitimate validator (Mišić et al, 2024).

3.19 Ponzi Schemes

Ponzi schemes is a fraudulent activity of which scammers generates returns for earliest investors using the money deposited from later investors. This scheme has reported in cryptocurrency exchanges markets as well (Virginia, 2024). The cryptocurrency wallet is regarded as another ponzi schemes of which it relies on the potential new buyers to buy the coin at higher prices and sooner the market would run out of new buyers which will make the price to remain constant Radanliev, 2024 and Peter & Gabriela, 2024). Most crypto-wallet owner are attracted by the presence of price volatility to have capital gains.

3.20 Fake Crypto Market

The presence of decentralized blockchain based crypto-market has attracted scammers and hacker to lure the potential services users into their fake market. Most cryptocurrency exchange markets advertised in social media are fake crypto-markets that tries to scams potential customers into their traps (Sangal et al, 2024). The fake market including the phishing websites, which comprises of fake websites, malicious ads, and imitated websites which traps its users towards fake-crypto market.

3.21 Cross-Site Scripting (XSS) and Request Forgery (CSRF)

Cross-Site-Request-Forgery (CSRF) attack is an attack that tricks the user to execute unwanted web application request while Cross-Site Scripting (XSS) attack is a kind of attack of which the malicious script is injected into the codes of legitimate website (Chimuco et al, 2023). The attackers force the victim to trigger the XSS codes by sending malicious link to be opened. The victims of this attack would compromise their financial information including cryptocurrency wallet information. Scammers

http://.doi.org/10.46792/fuoyejet.v9i4.4 engineering.fuoye.edu.ng/journal

uses CSRF/XSS attack to obtain a cryptocurrency wallet login detail from the victim's pages (Ivanov et al, 2021). The prevention techniques against CSRF and XSS attacks has been on the researchers table in several years. The attackers have been constantly changing different techniques to attack the victims (Khodayari et al, 2024). Sometimes prevention of XSS has been difficult to implement but detection and repair could be the only choice to mitigate these attacks (Shankar et al, 2024).

4. Results and Discussion

The Cryptocurrency wallets can be classified into three main categories. The first category consists of safe storage tricky wallets, where cryptocurrencies are stored securely on a personal device this is the safest method. The second category comprises of hot wallets, such as Metamask and TrustWallet which is the software-based crypto-wallets accessed through internet which are vulnerable to security threats and the third category is the exchange wallets, such as Coinbase Wallets which is provided by Centralized exchanges systems (Radanliev, 2024). The second and third types of wallets are the most vulnerable to the security threats.

The study has found that these crypto-wallets are susceptible to both general internet security vulnerabilities and blockchain based security vulnerabilities.

4.1 General Security Vulnerabilities

There are numerous security vulnerabilities which has been affecting the cryptocurrency wallet. These includes identity theft, ransomware, phishing, deanonymization, denial of service attack, channel amplification attack, mining malware, SIM swapping, SQL injection, Ponzi schemes, fake crypto market, cross-site scripting, and cross-site request forgery. These attacks and scams have been affecting the internet world in several years. The attackers would deploy several security vulnerabilities either to acquire the access of the user's computer or to block the access of the victim's computers. They would acquire the restricted access and compromise the victim's information so as to conduct cybercrime. Sometimes attackers would block the access of your own device and ask for the ransom. These general vulnerabilities can be divided into three groups:

Group-1: First group including the intentional scams such as identity theft, fake crypto-market, and Ponzi schemes of which the victims are lured to some fake services and compromise their identity or convinced to join some fake investments schemes for the hope of huge returns. The victims in this case are willingly share their wallet information or performs cryptocurrency transactions to invest in fake business. This kind of vulnerabilities will never end but it can be minimized by the presence of awareness among users. If the general public are reporting their incidences frequently it would decrease the number of new victims every day.

Group-2: This group including those scams and attacks such as phishing, ransomware, mining malware, SQL injections, cross-site scripting, and cross-site request forgery. In this category the victim's devices or website is subjected to malware and services are rendered or secret information is accessed in the background. To avoid these vulnerabilities the users required to deploy vulnerability scans periodically, or updating security breaches, and uses artificial intelligence (AI) vulnerabilities detection and prevention technologies that would help to fend away any attacks.

Group-3: In this category there are attacks such as denial of service (DoS) attacks, and Channel Amplification attacks. These attacks fabricate requests to overwhelming the website or devices capacity to block outs any legitimate communications. There are several AI techniques deployed to fend away such attacks. These include deployment of deep learning techniques which would uses AI to detect and prevent such attacks.

4.2 Blockchain Systems Security Vulnerabilities of Crypto-Wallet

The blockchain systems is a decentralized distributed ledger systems which require no third party to validate and authorize transactions. The smart contracts are used as a consensus mechanism before execution of transactions. The absence of a controlled central authority has been used as a vulnerability by the crypto-scammers. The wallets are susceptible to deanonymization attacks, long-range attacks, mining malware, Defi hacks, SLAM attack, double-spending attack, majority attack, eclipse attack, sybil attack, BGP hijacking attack, Liveness attack, Balance attack, and Adversarial attacks. The block chain systems would be vulnerable to these attacks so long as it remains decentralized because the attackers have been constantly changing the way to skip the detections and bypass any security measures imposed by the users. The weakness in network protocols architecture also has been used by the attackers to perform some attacks such as BGP hijacking, and SLAM Attack. The usage of AI to detect and prevent these kinds of attacks could help to minimize its impact.

4.3 Vulnerabilities Prevention Techniques

Since cryptocurrency wallets has been vulnerable to those kinds of attacks discussed in this research, there has been suggestions in place to mitigate its impacts. These detections and preventions techniques include introduction of Cyberbiosecurity, setup security requirements, adopt Cyber Insurance, deploy Expert System for Security Assessment, and adopt AI for detections and preventions for all vulnerabilities.

Cyber-biosecurity: In this scenario Cyber-Physical Systems (CPS) which is the collections of physical sensors and computer components integrated together to ensure safe operations. It includes sensing devices, data processing control which is connected to cyberspace to monitor, control, and prevents and cybercrime (Shankar et al, 2023).

Setup Cybersecurity Requirements: The organizations have to setup rules and principles regarding the systems usage to safeguard the systems against any security threats such as requirements for data processing,

http://.doi.org/10.46792/fuoyejet.v9i4.4 engineering.fuoye.edu.ng/journal

privacy, data transfer, and third-party services which would help to perform security scans periodically in case of any breach (Alghamdi et al, 2024).

Adopt Cyber-Insurance: The adoption of cyber insurance would help to gain users confidence in the usage of such services. The insurance company would help to force customers to adopt all security measures to be eligible for any damage incase of any security attacks.

Expert System for Security Assessment: Deployment of expert systems for security assessment would enforce several methodologies to be used against the penetrations techniques, threats model, and attack plans. This would set the knowledge base concerning threats and risks assessment techniques that can implements in the organization security policies (Silvestri, 2023).

5. Conclusion and Reconmendatios

5.1 Conclusion

The crypto-wallet security vulnerabilities are endless war against hackers and scammers. It needs frequently updated secured systems, technological awareness of presence of such threats, adoptions of updated security policies, and usage of Cyber-Insurance services. These are just mitigating techniques that would never eliminate these vulnerabilities from being utilized by the scammers but instead would minimize the impacts conceived by the individual customers or entities. The articles have articulated that crypto-wallet born by the exchange firms are the most vulnerable followed by the hot wallets which is software-based crypto-wallets accessed through internet.

5.2 Recommendations

There are several articles addressing the wallet security. Most of them attack common definitions of attacks causes, detections, and prevention techniques for example most attacks on blockchain systems could lead to double spending incurred in cryptocurrency. There are debates of whether the double spending is attacks or is the results of attacks. Therefore, this study recommends further studies to bring common understanding of all contracting security terminologies. Also, the study recommends crypto-wallets should be kept on individual storage devices and discourages any form of storages that would end-up on the exchange firms as they are most vulnerable to attacks.

References

Adeniyi, P. A., Ish Abhishta, A., Joosten, R., Dragomiretskiy, S., & Nieuwenhuis, L. J. (2019, February). Impact of successful ddos attacks on a major crypto-currency exchange. In 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP) (pp. 379-384). IEEE. DOI: https://doi.org/10.1109/EMPDP.2019.8671642

Achary, K., Nachiket, N. K., Adarsh, D., Prashanth, M., & Prathima Mabel, J. (2023). DDOS ATTACK DETECTION ON BITCOIN ECOSYSTEM USING DEEP LEARNING. International Research Journal of Modernization in Engineering Technology and Science. e-ISSN: 2582-5208. Volume:05/Issue:06/June-2023. DOI : https://www.doi.org/10.56726/IRJMETS42271.

Ahmad, M., Younis, T., Habib, M.A., Ashraf, R., Ahmed, S.H. (2019). A Review of Current Security Issues in Internet of Things. In: Jan, M., Khan, F., Alam, M. (eds) Recent Trends and Advances in Wireless and IoT-enabled Networks. EAI/Springer Innovations in Communication and Computing. Springer, Cham. ISBN: 978-3-319-99966-1. DOI: https://doi.org/10.1007/978-3-319-99966-1_2

Alam, M., Shahid, M. & Mustajab, S. (2024). Security challenges for workflow allocation model in cloud computing environment: a comprehensive survey, framework, taxonomy, open issues, and future directions. J Supercomput. DOI: https://doi.org/10.1007/s11227-023-05873-1

Albshaier L, Almarri S, Hafizur Rahman MM. (2024). A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions. Computers. 2024; Volume (13) PP: (1):27. DOI: https://doi.org/10.3390/computers13010027

Alghamdi, F. S., & Nor, R. B. M. (2024). Assessing E-commerce Adoption Determinants in Saudi Arabia: Impact of Financial Loss and Identity Theft. International Journal of Religion, Volume-5(Issue-1), PP: 368-379. DOI: https://doi.org/10.61707/96gazw11

Alhazmi, H.E., & Eassa, F.E. (2022). BCSM: A BlockChain-based Security Manager for Big Data. International Journal of Advanced Computer Science and Applications. DOI:10.14569/ijacsa.2022.0130364. Corpus ID: 247965213.

Angafor, G.N., Yevseyeva, I. & Maglaras, L. (2024). Securing the remote office: reducing cyber risks to remote working through regular security awareness education campaigns. Springer: International Journal of Information Security. (2024). https://doi.org/10.1007/s10207-023-00809-5

Anitha, C., Nalina, E., Sivaprakash, T., & Indumathi, G. (2024, January). Machine learning methods of sleuthing malevolent web channels. In AIP Conference Proceedings (Vol. 2802, No. 1). AIP Publishing. DOI https://doi.org/10.1063/5.0185199

Baninemeh, E., Jansen, S., & Labunets, K. (2024). A Security Risk Assessment Method for Distributed Ledger Technology (DLT) based Applications: Three Industry Case Studies. arXiv :2401.12358.

Bartoletti, M., Lande, S., Loddo, A., Pompianu, L., & Serusi, S. (2021). Cryptocurrency scams: analysis and perspectives. Ieee Access, 9, 148353-148373. DOI: https://doi.org/10.1109/ACCESS.2021.3123894.

Biryukov, A., & Tikhomirov, S. (2019, June). Deanonymization and linkability of cryptocurrency transactions based on network analysis. In 2019 IEEE European symposium on security and privacy (EuroS&P) (pp. 172-184). IEEE. DOI: https://doi.org/10.1109/EuroSP.2019.00022

Bleeping Computer (2024). New SLAM attack steals sensitive data from AMD, future Intel CPUs. Online, available from https://www.bleepingcomputer.com/news/security/new-slam-attack-steals-sensitive-data-from-amd-future-intel-cpus/ [accessed on 01/02/202

Carlisle, D. (2023). The Crypto Launderers: Crime and Cryptocurrencies from the Dark Web to DeFi and Beyond. John Wiley & Sons.

Chao, D., Xu, D., Gao, F., Zhang, C., Zhang, W., & Zhu, L. (2024). A Systematic Survey On Security in Anonymity Networks: Vulnerabilities, Attacks, Defenses, and Formalization. IEEE

Communications Surveys & Tutorials. ISSN: 1553-877X, DOI: https://doi.org/10.1109/COMST.2024.3350006

Chimuco, F. T., Sequeiros, J. B., Lopes, C. G., Simões, T. M., Freire, M. M., & Inácio, P. R. (2023). Secure cloud-based mobile apps: attack taxonomy, requirements, mechanisms, tests and automation. Springer: International Journal of Information Security. (2023) 22:833–867. DOI: https://doi.org/10.1007/s10207-023-00669-z.

CVEDetails.com (2024). Security Vulnerabilities, CVEs, Published In 2023, Online, available from https://www.cvedetails.com/vulnerability-list/year-2023/vulnerabilities.html [Accessed on 31/01/202

Darwish, D. (2024). Big Data and Cloud Computing. In D. Darwish (Ed.), Emerging Trends in Cloud Computing Analytics, Scalability, and Service Models (pp. 219-252). IGI Global. https://doi.org/10.4018/979-8-3693-0900-1.ch012

Deirmentzoglou, E., Papakyriakopoulos, G., & Patsakis, C. (2019). A survey on long-range attacks for proof of stake protocols. IEEE access, vol. 7, pp. 28712-28725, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2901858.

Dwivedi, R., Verma, M., Yadav, T., & Shukla, S. (2023, October). Pluggable Integrity Layer for Property Registration. In 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA) (pp. 396-403). IEEE. doi: https://doi.org/10.1109/BCCA58897.2023.10338893.

El Emary, I. M., & Yaghi, K. A. (2024). Machine Learning Classifier Algorithms for Ransomware Lockbit Prediction. Journal of Applied Data Sciences, 5(1), 24-32. DOI: https://doi.org/10.47738/jads.v5i1.161

Gans, J. S., & Halaburda, H. (2024). "Zero Cost" Majority Attacks on Permissionless Proof of Work Blockchains. Informs-Management Science Journal. https://doi.org/10.1287/mnsc.2023.02426.

Hafız Muhammad Raheed, Muhammad Zahid Hussain, & Rafia Jawed. (2024). DISINFORMATION AND CRIME: ANALYZING THE SPREAD OF FALSE NARRATIVES ON SOCIAL MEDIA IN PAKISTAN. International Journal of Contemporary Issues in Social Sciences .ISSN (E) 2959-2461 (P) 2959-3808, 3(1), 99–124. Retrieved from https://ijciss.org/index.php/ijciss/article/view/284

Houy, S., Schmid, P., & Bartel, A. (2023). Security Aspects of Cryptocurrency Wallets—A Systematic Literature Review. ACM Computing Surveys, 56(1), 1-31. DOI https://doi.org/10.1145/3596906

Ivanov, M. A., Kliuchnikova, B. V., Chugunkov, I. V., & Plaksina, A. M. (2021, January). Phishing attacks and protection against them. In 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) (pp. 425-428). IEEE.

Jover, R. P. (2020). Security analysis of SMS as a second factor of authentication. Communications of the ACM, Communications of the ACM Volume 63, Number 12 (2020), Pages 46-52. DOI: https://doi.org/10.1145/3424260

Khare, S., & Badholia, A. (2023). BLA2C2: Design of a novel blockchain-based light-weight authentication & access control layer for cloud deployments. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 283-294.

Khodayari, S., Barber, T., & Pellegrino, G. (2024, May). The Great Request Robbery: An Empirical Study of Client-side Request Hijacking Vulnerabilities on the Web. In Proceedings of 45th IEEE Symposium on Security and Privacy.

Kim, M., Suh, J., & Kwon, H. (2022, August). A Study of the Emerging Trends in SIM Swapping Crime and Effective Countermeasures. In 2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD) (pp. 240-245). IEEE.

Kish, S. P., Thapa, C., Sayat, M., Suzuki, H., Pieprzyk, J., & Camtepe, S. (2024). Mitigation of Channel Tampering Attacks in Continuous-Variable Quantum Key Distribution. ARXIV Journal :2401.15898. DOI: https://doi.org/10.48550/arXiv.2401.15898

Kumar Sharma, P., Gosain, D., & Diaz, C. (2023). On the Anonymity of Peer-To-Peer Network Anonymity Schemes Used by Cryptocurrencies. In The Network and Distributed System Security Symposium. Internet Society. ISBN 1-891562-83-5. DOI: https://dx.doi.org/10.14722/ndss.2023.23241

Li, S., Shi, S., Xiao, Y., Zhang, C., Hou, Y.T., Lou, W. (2024). Bijack: Breaking Bitcoin Network with TCP Vulnerabilities. In: Tsudik, G., Conti, M., Liang, K., Smaragdakis, G. (eds) Computer Security – ESORICS 2023. ESORICS 2023. Lecture Notes in Computer Science, vol 14346. Springer, Cham. https://doi.org/10.1007/978-3-031-51479-1_16

Li, W., Bu, J., Li, X., Peng, H., Niu, Y., & Zhang, Y. (2022). A survey of DeFi security: Challenges and opportunities. Journal of King Saud University-Computer and Information Sciences, Volume 34, Issue 10, Part B, 2022, Pages 10378-10404, ISSN 1319-1578, DOI: https://doi.org/10.1016/j.jksuci.2022.10.028.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future generation computer systems, Elsevier Volume 107, 2020, Pages 841-853, ISSN 0167-739X, DOI: https://doi.org/10.1016/j.future.2017.08.020.

Lokendra Vishwakarma, Debasis Das, Sajal K. Das, and Christian Becker. 2024. SmartGrid-NG: Blockchain Protocol for Secure Transaction Processing in Next Generation Smart Grid. In Proceedings of the 25th International Conference on Distributed Computing and Networking (ICDCN '24). Association for Computing Machinery, New York, NY, USA, 174–185. https://doi.org/10.1145/3631461.3631554

Lone AN, Mustajab S, Alam M (2023) A Comprehensive study on cybersecurity challenges and opportunities in the IoT world. Wiley Online Library, Secur Priv 6(6): e318

Mirza, D., Rahulamathavan, Y. (2023). Security Analysis of Android Hot Cryptocurrency Wallet Applications. In: Hewage, C., Rahulamathavan, Y., Ratnayake, D. (eds) Data Protection in a Post-Pandemic Society. Springer, Cham. https://doi.org/10.1007/978-3-031-34006-2_3

Mišić VB, Naderi Mighan S, Mišić J, Chang X. Decentralization Is Good or Not? Defending Consensus in Ethereum 2.0. Blockchains. 2024; 2(1):1-19. https://doi.org/10.3390/blockchains2010001

Mitre Corporation (2024). The mission of the CVE® Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. Online, available at https://cve.mitre.org/ [Accessed on 31/01/202

Morris, C., Herzberg, A., Wang, B., & Secondo, S. (2024). Bgp-isec: Improved security of internet routing against post-rov attacks. Network and Distributed System Security (NDSS) Symposium 2024, 26 Feb - 1 March 2024, San Diego, CA, USA ISBN 1-891562-93-2 https://dx.doi.org/10.14722/ndss.2024.241035

Nanda, M., & Goel, S. (2024). URL based phishing attack detection using BiLSTM-gated highway attention block convolutional neural network. Multimedia Tools and Applications, Springer PP (1-31). DOI: https://doi.org/10.1007/s11042-023-17993-0

Navaneethakrishnan, T., Manoharan, C., & Srinivasan, V. (2023). A

Study on Phishing Attacks and Its Legal Remedies (October 23, 2023). Indian Journal of Law and Legal Research, Available at SSRN: https://ssrn.com/abstract=4649005 or http://dx.doi.org/10.2139/ssrn.4649005

Norouzi Cholcheh, H., & Niksefat, S. (2024). A New Mixing Scheme to Improve Privacy in Bitcoin Cryptocurrency Transactions. Biannual Journal Monadi for Cyberspace Security (AFTA), 12(2), 16-23.

Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. I. (2024). COMPREHENSIVE REVIEW ON CYBERSECURITY: MODERN THREATS AND ADVANCED DEFENSE STRATEGIES. Computer Science & IT Research Journal, 5(2), 293-310. https://doi.org/10.21203/rs.3.rs-3909256/v1

O'Kane, P., Sezer, S. and Carlin, D. (2018), Evolution of ransomware. Wiley Online Library: Journal of IET Networks., 7: 321-327. https://doi.org/10.1049/iet-net.2017.0207

Parthiban, A. V., Rajeswari, D., & Ravichandran, P. (2024). Ideation Platform With Security Policies and Facial Mapping Feature. In AI Tools and Applications for Women's Safety (pp. 210-218). IGI Global.

Pathare, G., Patil, R., and Goel, P. (2022). Preventing Identity Theft using Blockchain Technology. International Journal for Research in Applied Science & Engineering Technology (IJRASET), ISSN: 2321-9653; IC Value: 45.98; Volume 10 Issue VI June 2022. DOI: https://doi.org/10.22214/ijraset.2022.44813.

Pavithran, D., Angeles, E., Shibu, C., & Shaikh, M. (2021, November). Attacks on Permissioned Blockchain for IoT. In 2021 4th International Conference on Signal Processing and Information Security (ICSPIS) (pp. 25-28). IEEE. DOI: https://doi.org/10.1109/ICSPIS53734.2021.9652429.

Peter J. and Gabriela P. (2024), Bitcoin, 2022, Crash (January 19, 2024). Elsevier. Available at SSRN: https://ssrn.com/abstract=4700061 or http://dx.doi.org/10.2139/ssrn.4700061

Popchev, I., Radeva, I., & Dimitrova, M. (2023, October). Towards blockchain wallets classification and implementation. In 2023 International Conference Automatics and Informatics (ICAI) (pp. 346-351). IEEE. DOI: https://doi.org/10.1109/ICAI58806.2023.10339101

Radanliev, P. (2024). The rise and fall of cryptocurrencies: defining the economic and social values of blockchain technologies, assessing the opportunities, and defining the financial and cybersecurity risks of the Metaverse. Financial Innovation, 10(1), 1. Springer: Financ Innov 10, 1 (2024). https://doi.org/10.1186/s40854-023-00537-8

Rai, B.K., Dubey, V. & Dubey, K. (2024). Blockchain based E-procurement system in healthcare. Health Serv Outcomes Res Method. https://doi.org/10.1007/s10742-023-00321-2

Rao, B., & Suvarna, S. G.(2023). TRUST & SECURITY ISSUES IN MOBILE BANKING AND ITS EFFECT ON CUSTOMERS. International Research Journal of Modernization in Engineering Technology and Science. e-ISSN: 2582-5208. DOI : https://www.doi.org/10.56726/IRJMETS39238

Ryu, G., Choi, D. (2024). Detection of adversarial attacks based on differences in image entropy. Springer: Int. J. Inf. Secur. 23, 299–314 (2024). https://doi.org/10.1007/s10207-023-00735-6

Sangal, S., Duggal, G., & Nigam, A. (2024). Blockchain's double-edged sword: thematic review of illegal activities using blockchain. Journal of Information, Communication and Ethics in Society. Emerald Insight Journal of Information, Communication and Ethics in Society. ISSN: 1477-996X, https://doi.org/10.1108/JICES-04-2023-0061

Sarah Azouvi and Marko Vukolić. 2022. Pikachu: Securing PoS Blockchains from Long-Range Attacks by Checkpointing into Bit2coin PoW using Taproot. In Proceedings of the 2022 ACM Workshop on Developments in Consensus (ConsensusDay '22). Association for Computing Machinery, New York, NY, USA, 53–65. https://doi.org/10.1145/3560829.3563563

Sarah Azouvi, George Danezis, and Valeria Nikolaenko. 2020. Winkle: Foiling Long-Range Attacks in Proof-of-Stake Systems. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies (AFT '20). Association for Computing Machinery, New York, NY, USA, 189–201. https://doi.org/10.1145/3419614.3423260

Sayeed, S., & Marco-Gisbert, H. (2018). On the effectiveness of blockchain against cryptocurrency attacks. UBICOMM 2018. IEEE: The Twelfth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies. ISBN: 978-1-61208-676-7

Sayeed, Sarwar, and Hector Marco-Gisbert. 2019. "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack" Applied Sciences 9, no. 9: 1788. https://doi.org/10.3390/app9091788

Sekiguchi, N., & Tanaka, H. (2024). BGP hijack attack policy against AS topology map. Elsevier Journal of Internet of Things, V: 25, April 2024, 101059. ISSN 2542-6605, DOI: https://doi.org/10.1016/j.iot.2024.101059

Shankar, D. D., Azhakath, A. S., Khalil, N., Sajeev, J., Mahalakshmi, T., & Sheeba, K. (2023). Data Mining for Cyber Biosecurity Risk Management–a comprehensive review. Elsevier. Journal of Computers & Security, Volume 137, 103627. DOI: https://doi.org/10.1016/j.cose.2023.103627

Shankar, S. P., Gudadinni, S. M., & Mohta, R. (2024). A Comprehensive Study of Cyber Threats in the Banking Industry. In Strengthening Industrial Cybersecurity to Protect Business Intelligence (pp. 244-269). IGI Global. DOI: 10.4018/979-8-3693-0839-4.ch011

Sharad Mangrulkar, R., Vijay Chavan, P. (2024). Bitcoin. In: Blockchain Essentials. Apress, Berkeley, CA. Online ISBN 978-1-4842-9975-3 DOI: https://doi.org/10.1007/978-1-4842-9975-3_3.

Shukla, A., Katt, B. & Yamin, M.M. (2023). A quantitative framework for security assurance evaluation and selection of cloud services: a case study. International Journal of Information Security-Springer. Volume 22, pages 1621–1650, (2023). DOI: https://doi.org/10.1007/s10207-023-00709-8.

Silvestri S. et el (2023) Cyber threat assessment and management for securing healthcare ecosystems using natural language processing. Springer: International Journal of Information Security (2024) 23:31–50 https://doi.org/10.1007/s10207-023-00769-w

Herskind, P. Katsikouli and N. Dragoni (2020), "Privacy and Cryptocurrencies—A Systematic Literature Review," in IEEE Access, vol. 8, pp. 54044-54059, 2020, doi: 10.1109/ACCESS.2020.2980950.

Sommervoll, Å.Å., Erdődi, L. & Zennaro, F.M. (2024). Simulating all archetypes of SQL injection vulnerability exploitation using reinforcement learning agents. Springer: Int. J. Inf. Secur. 23, 225–246 (2024). https://doi.org/10.1007/s10207-023-00738-3

Subashini, K., & Narmatha, V. (2024). Deep Learning Empowered Phishing URL Detection: An Exhaustive Approach. International Journal of Intelligent Systems and Applications in

Engineering, 12(14s), 213-222.
Suratkar, S., Shirole, M., & Bhirud, S. (2020). Cryptocurrency wallet: A review. In 2020 4th international conference on computer, communication and signal processing (ICCCSP) (pp. 1-7). IEEE. DOI: https://doi.org/10.1109/icccsp49186.2020.9315193
Tapsoba, W. C., Bassole, D., Kafando, R., Kabore, A. K., Sabané, A., & Bissyandé, T. F. (2024). Cyber Threat's detection using Machine Learning Algorithms. Hal. Science hal-04425411 , version 1 (30-01-2024)
Tyagi, A. K. (2024). Blockchain and Artificial Intelligence for Cyber Security in the Era of Internet of Things and Industrial Internet of Things Applications. In AI and Blockchain Applications in Industrial Robotics (pp. 171-199). IGI Global. DOI: https://doi.org/10.4018/979-8-3693-0659-8.ch007
Virginia Franke Kleist (2024) Fraud and Criminality in Cryptocurrencies and Crypto Exchanges, Journal of Global Information Technology Management, 27:1, 91-93, DOI: 10.1080/1097198X.2023.2300183
Vistro, D. M., Hassan, T., & Ullah, Z. (2024, January). Ransomware malware: Attacks and preventions. In AIP Conference Proceedings (Vol. 2802, No. 1). AIP Publishing. https://doi.org/10.1063/5.0181756
Xie, H., & Yan, Z. (2024). SPCEX: Secure and Privacy-preserving Cryptocurrency Exchange. IEEE Transactions on Dependable and Secure Computing.
Xu, Y., Zheng, J., Düdder, B., Slaats, T., & Zhou, Y. (2024). A Two-Layer Blockchain Sharding Protocol Leveraging Safety and Liveness for Enhanced Performance. Network and Distributed System Security (NDSS) Symposium 2024:2310.11373. https://doi.org/10.14722/ndss.2024.24006
Ye, G., Wu, M., Hong, G., & Yang, M. (2023, July). Revealing and Analyzing the Visual Scams of Cryptocurrency Wallets. In Proceedings of the ACM Turing Award Celebration Conference-China 2023 (pp. 148-149). DOI: https://doi.org/10.1145/3603165.3607444
Zhang, S., & Lee, J. H. (2023). Double-spending with a sybil attack in the bitcoin decentralized network. IEEE transactions on Industrial Informatics, 15(10), 5715-5722. DOI: https://doi.org/10.1109/TII.2019.2921566
Zhou, L., Xiong, X., Ernstberger, J., Chaliasos, S., Wang, Z., Wang, Y., & Gervais, A. (2023, May). Sok: Decentralized finance (defi) attacks. (2023) IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023, pp. 2444-2461, DOI: https://doi.org/10.1109/SP46215.2023.10179435.