11

Emerging Technologies and Cyber Security

Alka Vaidya

11.1. Introduction

For around three decades, Internet has become an essential part of global communication and directly or indirectly it has been integrated with people's lives around the world. Today, almost all types of organisations across verticals are using this widespread interconnected technology and have become a very much part of the cyber space. While different aspects of our lives are nearly intertwined with the cyberspace, any instability or insecurity in the same is bound to pose a lot of challenges. The technology is making our lives convenient, and yet it is also raising concerns about various crimes that are taking place in the cyber space.

The Indian banking sector has widely adopted internet and related communication technologies and has transformed India's digital landscape over a last decade. With the confluence of technological development, adoption of smartphones, improved data connectivity and progressive regulatory policies, the country has seen unprecedented growth in digital transactions. Simple and convenient payment modes such as Immediate Payment Service (IMPS), Bharat Interface for Money-Unified Payments Interface (BHIM-UPI), Pre-aid Payment Instruments (PPIs), etc., have helped India lead the world with a share of 40% global real-time payments being made digitally in 2021 (Das,2022).

Although, this unprecedented growth in digitisation is helping banks in offering cashless and convenient service to their customers, it is also raising concerns about various cyber-attacks resulting in data breaches or siphoning of funds. In last few years, not only number of attacks have gone up substantially, but the attack complexity and sophistication have also increased to a great extent. Today, banks are reasonably able to manage common threats such as viruses, keyloggers etc. with established security solutions. However, the traditional security solutions cannot protect them from more complex and custom-built attacks. In this scenario, banks need to adopt innovative ways to combat the new-age cyber-attacks where technologies like Artificial Intelligence (AI), Machine Learning (ML) and Blockchain provide a promising future. These key technologies are likely to drive the next wave of digital transformation and they also have potential to bolster cyber security preparedness of banks.

On the flip side, AI and blockchain are not panacea to every security problem nor are they impervious to cyber-attacks. Today, hackers are successful both in hacking blockchain based cryptocurrency platforms or launching an AI-driven cyber-attack against organisations. With this as a background, this chapter focuses on the opportunities and challenges of AI/ML and blockchain technology in the field of cyber security. It elaborates on how banks can leverage the features of AI/ML and blockchain in enhancing their cyber security posture and at the same time, what new threats are being faced with their adoption.

The chapter is organised as follows: The second section highlights few large-scale cyber-attacks faced by Indian banks and the evolving threat landscape. It also describes various regulatory and government initiatives in cyber security management. The third section gives background of AI/ML, its role in cyber defence and the opportunities it gives to hackers. The fourth section describes blockchain properties and its relevance to cyber security, few use cases of blockchain in security domain and various types of attacks that have happened on its widely used application, viz. cryptocurrency. The final section summarizes the discussions.

11.2. Cyber Attacks on Indian Banks

One of the important reasons for banks being targeted by attackers is that they handle vast amount of sensitive customer and financial information. The recent government data confirms the sharp rise in attacks on the banking sector (Ohri, 2022). In August 2022, the central government notified the Parliament that between 2018 and 2022, Indian banks recorded 248 successful data breaches of which 41 were reported by public sector banks, 205 by private sector banks, and 2 by overseas banks. The incidents of malware (malicious software) and ransomware are also on the rise. The Indian Computer Emergency Response Team (CERT-In) observed a 51 percent increase in ransomware incidents in the country in the first half of the business year 2022 (Sur, 2022).

Illustrative Examples of Cyber Attacks on Indian Banks and Payment System Providers

In recent times, we have seen several high profile cyber-incidents both in India as well as globally. Few such examples from Indian banking sector are mentioned below:

1. 3.2 million debit card data was compromised between May and July 2016, and it was not until September, the banking system was aware of this large scale hack. The sophisticated malware was injected into the systems of Hitachi Payment Services and it remained undetected and concealed during this period.
2. In Union Bank of India, hacker tried to swindle $171 million from the USD Nostro account of the bank, but the bank could get the money trail and recover it subsequently (2016).
3. City Union Bank suffered a cyber hack when hacker hacked into their system and transferred nearly $2 million via SWIFT to overseas banks in three transactions of which they could block one worth $0.5 million. (2018).
4. Cosmos Bank, Pune - a well-planned and highly-coordinated operation that focused ATM and SWIFT infrastructure of the bank and the loss was around $13.5 million. (2018)
5. Telangana State co-operative Apex Bank faced fraudulent transactions which siphoned off Rs. 1.96 Crore (2021)
6. With the help of sophisticated hacking tools hackers hacked into servers of Hyderabad based AP Mahesh Bank and Rs 12 Crore were siphoned off (2021-22).
7. CashMama, an Indian money lending platform, (now defunct), suffered a data breach that exposed the customer details such as full names, dates of birth, home address, bank account details, etc. (2022)
8. Hackers stole Rs 7.3 Crore worth of funds in 831 transactions over a period of 3 months from online payment gateway company Razorpay. (2022)

The attacks mentioned above have resulted in various risks for banks such as breach of customer data, business disruption, loss of reputation, post-breach cost of overhauling systems and processes, penal actions from regulators, etc. Such risks, if not managed proactively, may turn into 'systemic cyber risk' (Forescey, 2022). Especially, smaller banks are more susceptible to systemic cyber risk if they further digitize their operations and do not take into considerations the underlying cyber threats.

Regulatory/Government Initiatives in Enhancing Cyber Security in Banks

The Reserve Bank of India (RBI) has taken several initiatives to address cyber security issues in order to improve overall cyber resilience of banks. The RBI has issued comprehensive guidelines on ‘Cyber Security Framework’ to Banks in 2016 for implementing next-generation cyber defence capabilities. In 2019, similar guidelines were also issued to Urban Co-operative Banks. From time to time RBI has issued circulars, guidelines, awareness booklets such as:

- Cyber Security Controls for Third party ATM Switch Application Service Providers (2019)
- Master Direction on Digital Payment Security Controls (2021)
- Booklet on Modus Operandi and Precautions to be taken against Fraudulent Transactions – Banks (2022)
- Consumer Awareness - Cyber Threats and Frauds (2022)

The Government of India has also taken numerous initiatives in this regard, some of which are listed below:

- Indian Computer Emergency Response Team (CERT-In) has been operational since 2004 as a national agency for cyber security incident response.
- Cyber security awareness campaign on ‘beware and be aware of financial frauds’ is jointly conducted by CERT-In, RBI on the Digital India Platform.
- National Critical Information Infrastructure Protection Centre, was established in 2014, to monitor and forecast national-level threats to Critical Infrastructure including banks and to issue policy guidance, expertise sharing and situational awareness for early warning or alerts.
- “Cyber Swachhta Kendra” to provide detection of malicious programs and tools to remove the same.
- The new Personal Data Protection Bill (2022) when gets passed, would establish a legal framework about appropriate usage and protection of collected data by the Data Fiduciaries (such as banks).

The Changing Nature of Cyber Threats

In most of the attack examples above, one common concern is that, the final heist (or data loss) is not a result of a single, isolated incident such as malware or phishing email. On the contrary, the attackers have been able to carry out a series of tasks over a few days or months without getting noticed by the security solutions used by those organisations.

As the global internet traffic is on the rise, security analysts are finding it difficult to monitor the data volumes coming from several sources or detecting abnormal network behaviour, if any. With complex networks, it has become easier for hacker to successfully enter into a corporate network and pretend to be an internal employee, bypassing all external defences.

Banks cannot rule out the possibility of malicious insiders including staff or a vendor representative who would abuse their credentials to either leak the personally identifiable information of customers or to simply sabotage the systems due to past grudge against the organisation.

Another area of concern is customised malware that hackers keeps modifying to evade detection by traditional security technologies. A standard malware detection tool uses “signature based” approach where known malware samples are stored in a database against which the signs are matched. No doubt, such tools are industry-tested and effective against the known threats, but they cannot detect unknown malwares.

Today, financially or ideologically motivated hackers go after specific targets, especially aiming at the data breach. Such an attack is more persistent in nature in which an attacker targets a specific organisation, enters into their system, remains undiscovered for longer period of time and ultimately sends out the data to his/her desired servers. This phenomenon, commonly known as Advanced Persistent Threats (APT) usually exploits vulnerabilities that are not yet known to the public and cyber security community (a ‘zero-day’ vulnerability).

For the traditional intrusion detection systems it is always challenging to notice such an attack, due to its obfuscated nature.

Lastly, today, organisations are using tens of thousands of devices, but they have limited number of skilled professionals in their security operation centres. So, it is practically impossible to attend to thousands of security alerts received from their threat detection and monitoring solutions.

In this evolving threat landscape, technologies like AI and ML present a great opportunity as they can automate data gathering from various sources, identify anomalies and continually learn and self-improve at a pace that's humanly not possible. Considering the fact that today's cyberattacks are innovative and persistent, traditional security technologies are facing several limitations when it comes to detecting them.

In the next section, we discuss the role of AI and ML in cyber security.

11.3. Artificial Intelligence and Machine Learning

Though Artificial Intelligence (AI) has become a buzzword today, the origins of AI can be traced to late 1950's, when researchers had a strong assumption that 'every aspect of learning or any other feature of intelligence can be so precisely described that a machine can be made to simulate it'. Nevertheless, AI has never had a smooth ride, some reports criticised developments in AI for various reasons. Few techniques such as neural network gained prominence in 80's, but fizzled out later.

However, in the last 10 to 15 years, industries have shown renewed interest in several AI based applications and many organisations including banks have adopted AI in various business applications. The factors such as availability of vast amount of digitised data (both in structured and unstructured formats), incredible rise in processing power, low-cost storage with cloud based technology and enhanced global connectivity have enabled industry adoption of AI. Worldwide, retail industries like telecomm, banking and e-commerce giants became some of the early adopters of AI and its sub-domains like robotic process automation, machine learning, analytics, etc.

Machine learning (ML) is the major component of today's AI systems. It is a set of techniques that allow machines to learn in an automated manner through pattern recognition rather than through explicit instructions from a human being. The techniques used in machine learning are broadly classified as: supervised, unsupervised, semi-supervised and reinforcement learning. In supervised learning the past data fed to the algorithm which always contains one column with the known outcome – usually called as 'label'. e.g. such data could be about whether the transaction is fraudulent or not, email is spam or genuine, etc. Using this dataset, the ML model is trained which is subsequently used to find the unknown labels of fresh dataset.

In unsupervised learning, the input dataset does not have a column with 'labels' and all columns are treated on par. From such datasets machines learn the pattern and break them down into groups usually known as clusters e.g. user-activity logs which may be huge in size, can be segmented into groups to identify suspicious user behaviour or outliers that are present. The semi-supervised models use both labelled and unlabelled data and preferred when there is a limited set of existing labelled data.

Reinforcement learning algorithms learn the best actions based on the concept of rewards and punishments. Such a learning model usually interacts with the environment and after observing the consequences of its actions, it learns to alter its behaviour (Arulkumaran et al., 2017). The new generation Intrusion Detection Systems (IDS) are using such techniques where by effectively learning from the environment they can identify network intrusion in an automated manner. (Alavizadeh H et al., 2021)

AI/ML Adoption by Indian Banks

As per the PWC survey (2022), 83% of Indian Financial Service institutions indicate that 'enhancing customer experience' is the top driver of deploying AI based use cases in their organisations. Most of the Indian banks are using AI/ML based applications in the areas like:

1. Customer service and engagement with the help of chatbots.
2. Automate business processes with software robotics.
3. Understanding patterns in customer behaviour accordingly give personalised offers
4. Payments fraud detection and prevention, identity verification associated with Anti-Money Laundering (AML) and Know Your Customer (KYC).

However, adoption of AI/ML in cyber security is relatively limited in Indian banks. Some of the leading public and private banks have started using security tools with certain ML algorithms. With the help of outsourced partners and system integrators, such banks have created (or in the process of creating) platforms like Security Orchestration, Automation and Response (SOAR) or Next Generation Security Operation Centre (SOC). These platforms provide them powerful cognitive capabilities to detect, mitigate and prevent threats by using ML techniques. But majority of the banks in India are yet to make a sound beginning as regards to deploying AI/ML use cases in cyber security domain.

AI-ML in Cyber Defence

In the field of cyber security, one of the early adoptions of machine learning technique was in the area of filtering spam emails. e.g. Gmail, Yahoo, Outlook, etc. have been using ML in spam filtering process for many years. Several ML techniques such as k-nearest neighbours, neural networks, deep learning are being used to detect spam filters. Such models have now advanced to a level where they can detect and filter spam emails with about 99.9 percent accuracy (Dada E et al., 2019).

In addition to spam detection, there are many other areas where use of AI, ML is relatively recent. The following table (Table 11.1) summarises various types of cyberattacks and what types of machine learning techniques are prevalent in detecting these attacks.

Key Lessons for Banks

It can be seen from Table 11.1 that, for the behaviour based detection, unsupervised or reinforcement ML techniques are more commonly used in the industry. There may be unusual behaviour exhibited by networks or by a user, e.g. sudden increase of data transfer in the network or unusual uploads of files by a certain user could be the indicator of an impending cyber-attack. In cases like these, user behaviour modelling and anomaly detection algorithms would help banks in recognising such exceptions at an early stage of attack.

One of the important challenges for banks today, is how to counter the attacks or identify the incidents that are totally new. In absence of historical "labelled" data, banks need to adopt unsupervised machine learning models. This would help them in finding patterns of behaviour and then check the outliers that represent possible anomalous or suspicious activities.

As described in Table 11.1, supervised ML techniques can also be used to detect cyber-attacks or to identify fraudulent card transactions. However, in the world of dynamic threat vectors, when banks need to do behaviour based predictions, unsupervised and reinforcement learning based threat prediction could be a more practical approach.

AI ML: Benefits to Hackers?

While AI/ML has huge potential in predicting or detecting the security related incidents, bad actors can also take advantage of this technology in several ways. AI based hacking methods may be more effective because of their ability to learn the present environment and predict what might happen in the future. e.g. AI powered malware can evade static defences such as firewall. By observing and predicting the actions by security teams, they can subtly and frequently modify certain indicators to cause harm. By sitting in the system such a malware may send out relevant data with low chances of detection.

A highly targeted and tailored "spear phishing" emails are more labour intensive to construct. Such spear phishing emails can be generated

TABLE 11.1

Machine Learning Techniques Used in Detecting Various Cyber-Attacks

Type of an Attack	*Description*	*Machine Learning Techniques used*
Zero Day attack detection	In this attack, the vendor/developer (of an operating system or a database, etc.) is either not aware of a flaw in his product or has not yet released the solution to fix the same.	Outlier-based detection using Deep Learning Approach (Hindy, 2020) Hybrid supervised approach as zero day attack features are similar to that of existing attack.(Guo, 2023)
Distributed Denial of Services (DDoS) Attack	Servers get flooded with malicious requests and legitimate users fail to access them.	Supervised Learning Classification Techniques like Logistic Regression, Naive Bayes (Kumari et al.,2022), Decision Trees -Random Forest to trace the DDoS Attack (Lakshminarasimman et.al. 2017) Hybrid/Semi-Supervised ML Learning Clustering technique applied first to distinguish normal and abnormal traffic, subsequently decision trees, KNN techniques are applied on labelled data. (Aamir and Zaidi, 2021)
Evasive Malwares	The malicious software that remain undetected by traditional signature based anti-malware tools by evading them.	Deep leaning based behaviour analysis of malwares along with dynamic analysis of API calls made by the malware is conducted. (Hisham, 2015) Association based classification and rule generation with iterative learning(Chandrasekar et al., 2012)
Phishing attacks	Attacker sends a fraudulent message (usually in email) to trick a victim into revealing his credentials.	NLP based detection of malicious, Phishing URLs (Buber et al, 2018) Phishing website detection with RNN (recurrent neural networks) (Datta, 2021)
Malicious email Attachments with MS office and ZIP archives	Malicious email attachment is an entry to the hacker in organisation network	Deep Neural Networks and Gradient Boosted Decision Trees (Rudd et al., 2018), Deep Reinforcement Learning (Muralidharan et al., 2023)
Internal Threats		
Unauthorised access	A malicious user may get access to systems as he/she is not given least privilege	Risk-Based Authentication- User behaviour prediction using Neural network (Jagannathan,2022)
Abnormal User Behaviour	- Abnormal Data Downloads - Source Code Theft - Stolen Credentials - Abnormal transaction pattern by the insider (clerk, teller, etc.)	Deep Learning based User Entity Behaviour Analysis (UEBA): Deep Reinforcement Learning and use of semi-supervised learning where real alerts are fed back to the system to fine tune the model and increase the efficiency of the model. UEBA gives an understanding of how users (humans) and entities (machines) normally behave and aggregates the anomalies per user and entity when it deviates from its normal behaviour (Shashank, 2016) User-behaviour anomaly detection is done with Convolutional Neural Network (CNN). (Wang,2017) NLP based sentiment analysis is done on email (subject line, sender, recipients, attachment, etc.)
Network Behaviour Analysis		
Network Behaviour and Anomaly Detection	As a result of DDoS attack or Malware infection network may display anomalous behaviour	Unsupervised Learning such as K-Means clustering can be applied on Data Packets and packet header to form the clusters and identify outliers(Chunfen B, 2018)
Lateral Movement on network during Advanced Persistent Threats (APTs)	In APT based attack, attacker remains persistent on the organisation network and can move closer to valuable assets (data) by escalating his privileges and without getting caught.	Unsupervised Learning: Clustering – grouping the network users based on their roles, entitlements and identifying outliers (Lah,2018) Clustering for detecting lateral movement of Malware over the network(Bhasin et al., 2018)

	Application Level Attacks	
SQL Injection	Attacker usually targets databases of websites by entering malicious code through input boxes provided in the web application. He may get hold of confidential data or may delete/alter the contents of the data tables.	Supervised Learning Techniques such as Logistic Regression, Decision Trees, SVM are used on data such as URL, user text input, text area, request header, etc.(Shaheed et al., 2022)
Cross-Site-Scripting	Malicious code is injected into a website which can send sensitive information to an attacker's web server	Supervised Learning techniques such as SVM, Decision trees, the Naive Bayes classifier, Logistic Regression based models.(Vishnu,2014) Multi-Layer Perception (MLP) Deep learning models are built using several URL features, the tags used, special keyword, redirections, etc.(Ayo et al, 2021)
Debit/Credit Card Fraudulent Transactions	Identifying fraudulent transaction on card (both card not present or present)	Supervised techniques like Random Forest, ANN, Logistic Regression (Ileberi, 2022)

by using "AI-as-a-Service" platform. A research experiment has shown that significantly higher number of people clicked the links of AI based spear phishing email than a human-written email. (Lim et al., 2020)

Criminals are using deep learning based fake audios and videos, commonly known as 'Deepfake' to carry out identity frauds. This technique uses facial mapping technology and AI that exchanges the face of a person on a video with the face of another person. Banks need to be careful about this, as it can be used for opening fake accounts.

If the security teams are using AI/ML models to identify breach attempts, they highly rely on correctly labelled data samples. However, such models are being poisoned with inaccurate data which could result in incorrect predictions.

Thus, today, industry is witnessing both 'defensive' and 'offensive' AI and hence security experts would need to fight 'AI' with 'AI' in days to come. It is imperative that banks need to automate their defence to disable AI based attacks. While machines deal with data crunching, skilled humans will play an important role to monitor and interpret AI's decision making.

11.4. Blockchain – A Distributed Ledger Technology (DLT)

The term 'blockchain' is no more unfamiliar in the context of banking technology. Since the publication of white paper on Bitcoin (2008), this technology has made immense impact across multiple industries such as healthcare, manufacturing, and government organizations. It is predicted to be the 'beating heart of finance' (Bruno, 2016).

In some ways, blockchain technology is similar to the internet which uses a decentralised network instead of a single server. Simply put, blockchain is a shared, replicated, add-only type of a database- where writing (or appending) is shared among the participants but validation must be performed by all the participants on that blockchain. With the help of cryptography-based distributed ledger, blockchain technology enables trusted transactions among untrusted participants in the network. Blockchain networks like Bitcoin are 'Public' networks where anyone can participate and it does not have a single entity controlling the network. Whereas, a 'Private' blockchain is managed by the central entity and participants on the network know each other. Though the original idea presented was about providing blockchain as a backbone to the world's first decetralised cryptocurrency, the other industries including banking have seen the potential of this platform for a variety of use cases beyond crypto.

Blockchain Adoption in Indian Banking Sector

Blockchain technology is being explored by many Indian banks in areas like trade finance, cross-border remittance and vendor financing. In 2021, fifteen Indian banks including the State Bank of India, three other public sector banks and eleven private/foreign banks have formed a consortium called Indian Bank's Blockchain Infrastructure Co (IBBIC) to digitise trade finance business process. Using a blockchain in trade finance, banks can avoide huge paperwork involved in it and blockchain would make it harder for a frauster to raise multiple Letters of Credit for the same good shipment.

In 2017, J P Morgan developed Quorum, a permissioned variant of Ethereum blockchain for enterprise solutions, which is used as Interbank Information Network(IIN). Seven Indian banks have joined IIN and aim to provide secure and fast exchange of information to facilitate cross-border payments in minimum time. (RBI 2020). The Reserve Bank of India has also been proactive in guiding banks for such developments through its regulatory sandbox environment.

As banks are pursuing their effort of using blockchain in business areas, they need to explore how decentralized, consensus-driven, immutable nature of blockchain makes it a sound use case in the area of cyber security. The following write-up describes how some of the inherent properties of blockchain would potentially help improve few areas of cyber security. It will also throw some light on the differing side and discuss the susceptibilty of blockchain to various types of cyber attacks.

Blockchain Technology and Cyber Security

Domain Name System on Blockchain

Traditionally, Domain Name System (DNS), which translates the domain names to machine readable IP addresses, has been operating on a centralised model and it is distributed across the world by several service providers. The current DNS system is vulnerable to certain methods of manipulation such as DNS hijacking or a redirection attack, which redirects user from the real location to a different, malicious, website. The Distributed Denial of Service (DDoS) attack is also a common phenomenon on today's DNS.

As against this, blockchain DNS is a decentralized DNS server that allows registering, managing, and resolving of domain names and related data exchanges without any centralised authority (Munene ,2022). In such implementations, the data such as domain name configurations could directly be distributed on a blockchain and entities involved (such as registries, registrars) could straightaway interact with this blockchain to manage the domain name. Some of the examples of such DNSs are: Ethereum Name Service (ENS), Handshake and Blockstack.

From cyber security point of view, blockchain DNS would bring certain advantages. Such a DNS, being decentralised and peer-to-peer network, it cannot be stopped. So, if there is a Distributed Denial of Service (DDoS) attack, it can be successfully mitigated and availability can be ensured 24/7. Such a DNS also uses the consensus protocol, and hence integrity of the data would be managed better, as it cannot be modified without consensus.

Blockchain for Digital Identities

Digital Identity (DID) is basically the digital representation of information relating to a particular individual, organization or device. Today, digital identities are no more restricted to usernames or email IDs, but they also include information such as individual's shopping preferences and website usage behaviour (Weston, 2022). Identity is an essential requirement for various tasks such as accessing banking service, government service, etc. Generally, traditional DID systems come with the burden of complicated paperwork processes and limited access. The existing state of digital identities has several challenges both for organisations and individuals. Such identities are usually stored by the organisations in centralised databases which might run on legacy software and it could be the prominent target for a hacker. This practice is also prone to identity frauds as users could manipulate different identities with the usernames and passwords for the websites as there is no standardized approach.

The blockchain based digital identity can solve many of these problems by focusing on the mechanisms such as identity management, decentralized identifiers, and embedded encryption. In this, the user needs to sign up for a self-sovereign-identity which would give him/her full ownership and control without relying on central authority. Such an identity would give a user single login for different platforms be it social media or e-commerce website.

Most importantly, from bank's point of view, this would simplify the KYC processes. At present, every bank or financial institution need to individually perform the KYC process and stores a digitized version. With digital identity being maintained on a shared ledger, after taking customer's consent, banks will be able to access relevant parts of the stored data and perform due diligence.

Blockchain for Cyber Threat Intelligence Sharing

Cyber Threat Intelligence (CTI) is the process of identifying and analysing cyber threats. It is the threat information that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for decision-making processes (NIST, undated). The primary purpose of this, is to help organisations to perceive the cyber risks in proactive manner and to make informed decisions regarding the response to those threats. The ability to exchange CTI in a secure manner and without compromising the privacy of participating entities is a big challenge for organisations at present.

A blockchain based threat intelligence platform can have various advantages. A decentralised threat information repository can avoid single point of failure and tampering of sensitive data. Blockchain can maintain account anonymity to maintain the privacy of CTI sharing party. By obtaining threat intelligence from blockchain, it is helpful to construct an attack chain, simulate the attack process, and then provide more accurate dynamic defence.

The banks which want to participate in such projects can on-board themselves on a decentralised trust network and leverage it to exchange respective threat indicators among the peers on the network. This would help the peers tune their defences against possible similar threats thereby avoiding the potential losses. Banks can also interact with various security agencies like CERT and NIST using such platforms.

Although, the dynamism of blockchain is helping cyber security domain, these blockchain based applications are not immune to cyberattacks. Especially, the most widely used application - 'cryptocurrency' has witnessed a few serious incidents in which victims world over have lost millions of dollars.

Attacks on Blockchain based Systems

In the recent past, security of blockchain-powered cryptocurrency has been questioned a lot due to numerous hacks and cyber-attacks on both crypto exchanges and individuals participants. Though exchanges have proliferated and become more advanced, as can be seen in Figure 11.1, many of them have become defunct after alleged hacks. Figure 11.2 represents the worldwide crypto heists till date (both value and volume) and shows the increasing trends with total fraud of about $9 billion (Tsihitas,2022).

With the rise in popularity of cryptocurrencies, today, cyber criminals are investing their time to find innovative ways to attack the underlying systems. Though it is extremely difficult to hack into blockchain per say, attackers are targeting the vulnerable spot in the surrounding systems to transfer/withdraw cryptocurrency. Some such attacks on cryptocurrencies have been described in the following part of the chapter.

Use Wallet Attacks

Consumers who invest in crypto often store their currency in a digital wallet in the form of a mobile app on their smartphones and just like any other app there are numerous ways to attack these apps. Unlike a physical wallet, crypto wallets technically don't store the currency. It remains on the blockchain, but can be accessed with the private key, stored in a wallet. Wallets in the context of cryptocurrencies is a place to store user's private key (somewhat similar to password which is known only to the owner). A public key (like a bank account number) or the "wallet address" is used to send and receive the money.

FIGURE 11.1

No of Platforms/Exchanges Affected

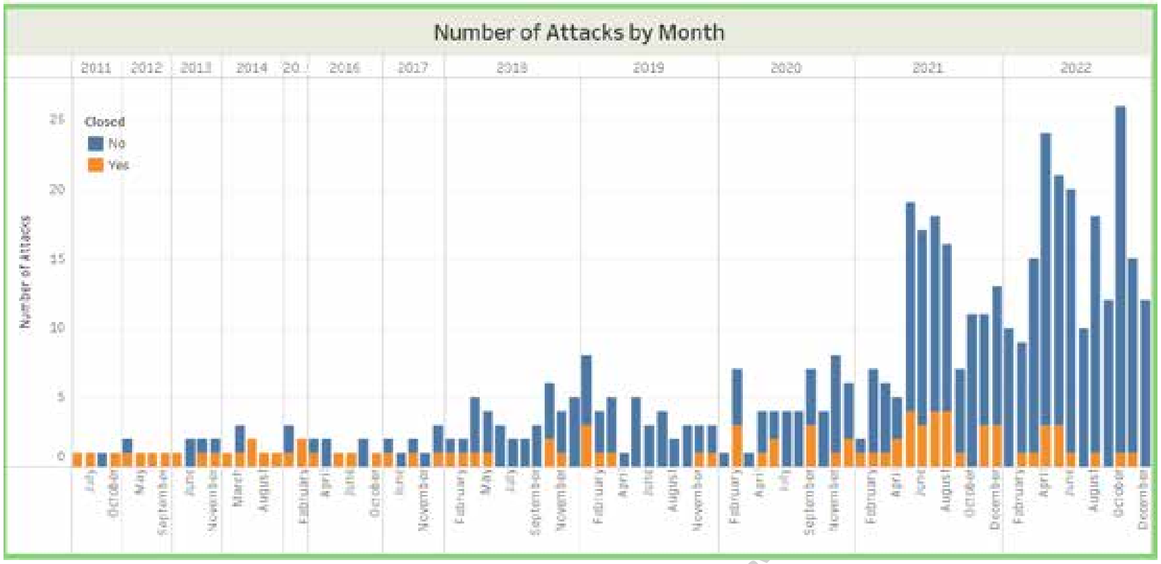
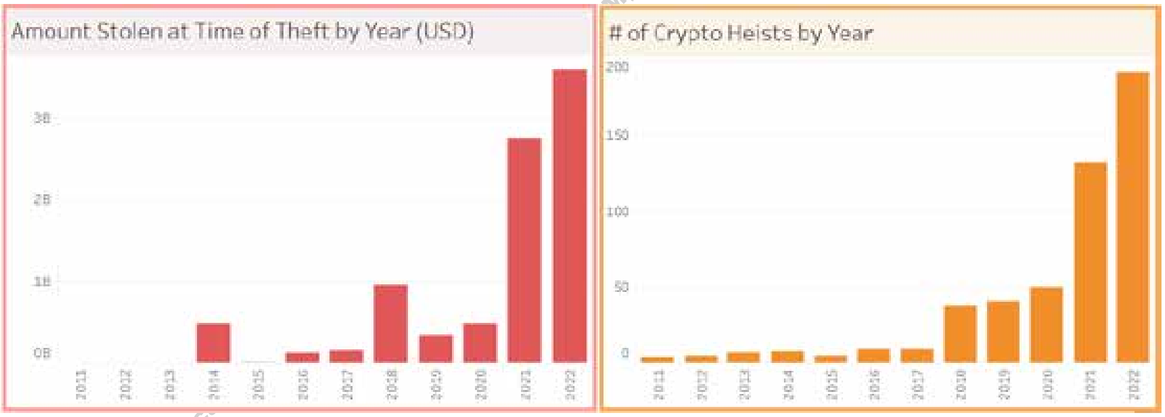


FIGURE 11.2

Crypto Heists in Value ($Bn) and Volume



Source: Comparitich.

To obtain wallet credentials (i.e. private key) attackers use both traditional methods like phishing, dictionary attacks, etc. or they apply sophisticated techniques to find out the vulnerabilities in cryptographic algorithms.

The wallets are classified under two main types: hot and cold wallets. A hot wallet (or a software wallet) is a form of digital storage or an app that you can access with your mobile phone or a computer, and is connected to the internet. As hot wallets are connected to the internet they are not as secure from hackers as their counterparts — cold wallets. A cold wallet (or a hardware wallet) is a physical device that keeps your cryptocurrency completely offline.

There are several ways in which these wallets can be attacked. A crypto wallet security vulnerability or any inadvertent malware download by the user can manifest into secret transfer of funds from wallets to unknown recipients. e.g. an Android malware 'Sharkbot' (of 2018) resurfaced in 2022 and it was found to have been downloaded by over 100,000 users. (Techdesk-Indian Express,2022) This malicious app was disguised as an app for trading cryptocurrencies on exchanges, such as Poloniex and Bittrex and it would trick users into granting them access to their login data.

Wallet users are also susceptible to traditional attacks like Phishing where a potential victim gets tricked into revealing sensitive information. In 2018, there was an attack on IOTA wallet. (Cimpanu, 2018) These wallets are initiated with an IOTA seed which is 81 characters long and similar to the private key. A hacker created a website IOTASEED.IO that looked very legitimate to new users. They trusted it and generated this seed. Then, when a user had used the seed to create a wallet, Iotaseed.io would use the seed to access a user's wallet without permission and steal the coins inside, quietly transferring them to another wallet address. As a result, in January 2018, more than $4 million worth of IOTA were stolen by the hackers from victims' wallets.

51% Attacks

When a single person or group of people gains control of over 50% of a blockchain network's validation power (mining power), it is called as 51% attack or a majority attack. This is usually achieved by hiring mining power from a third party. In the traditional sense, it is similar to the steps involved in finding mineral resources from mines, requiring huge amounts of energy, time and money to uncover something before others do. In this attack, the successful attackers gain the ability to tamper with transactions or to change the ordering of new transaction and forge blocks, by controlling 51% of the computing power of the entire network.

As a blockchain network grows and acquires news mining nodes the success rate of a 51% attack drops as the cost of performing a 51% attack rises significantly. On established and matured cryptos such as Bitcoin or Ethereum, the chance of such attacks is almost NIL as the financial costs would be so high that they would outweigh the benefits. But small cryptocurrencies are at risk of such attacks. In August 2020, 'Ethereum Classic' faced this attack where the attacker managed to reorganise 7000 blocks, or two days' worth of mining (etherchain_org, 2020).

DDoS Attacks on Blockchain Network

Traditionally, Distributed Denial of Service (DDoS) attacks are achieved by sending more traffic than the network can handle which overwhelms the underlying application. It is a popular belief that blockchain networks are immune to such attacks as a single node going down due to DDoS attack may not bring down the whole blockchain network. However, by flooding the blockchain with spam transactions, its availability for legitimate users goes down significantly. Most of the blockchains maintain a fixed capacity of blocks of a certain size at regular intervals. Anything in excess for the current block usually goes to memory pools and later it is considered for the next block. If an attacker floods many spam transactions, the genuine transactions would sit in memory pools and would not be added to the ledger.

DDoS, though, very difficult to execute on blockchain, it is not impossible. Cybercriminals look for network vulnerabilities and exploit them with the attacks like DDoS. In 2020, major crypto exchanges such as Bitfinex (Hong Kong) and OKEx (Malta) had suffered a massive DDoS attack. (Palmer, 2022)

Vulnerabilities in Smart Contracts

Smart contracts are simply programs stored on a blockchain and they are typically used to automate the execution of an agreement, without any intermediary's involvement or time loss. They are used to automate the workflow, triggering the next action when conditions are fulfilled.

Many blockchain attacks have happened due to certain vulnerabilities in a smart contract. There may be few weaknesses in smart contract which pose risks to the parties that sign the contract. For instance, bugs discovered in an Ethereum contract cost its owners around $70 million in 2016. It was using a language called 'Solidity' for implementing the smart contracts. It was targetted for a destructive attack – 'Re-entrancy'. It happens when the attacker empties funds from the target by continuously calling the target's withdraw function. Here, the contract fails to update the victim's balance and the attacker can continuously call the withdraw function to drain victim's account.

Central Bank Digital Currency (CBDC) and Cyber Threats

The concept of Central Bank Digital Currency (CBDC) has generated keen interest among central banks across the globe and India is no exception to this. The Reserve Bank of India, has already introduced the pilot project in the Digital Rupee – both in Wholesale (e₹-W) and Retail (e₹-R) segments in November and December 2022 respectively. CBDC is aimed to complement current forms of money and it is envisaged to provide benefits like more efficient payment systems and furthering financial inclusion. However, like existing payment systems CBDC ecosystem may also be vulnerable to cyber threats and hence the RBI has rightly acknowledged, 'Security has to be the prime design concern while designing CBDCs since inception'(RBI 2022).

The nature of risks may vary depending on the design considerations for CBDC . A blockchain or DLT based CBDC would require the involvement of third parties as validators of transactions and malicious validator nodes can pose security risks. On the other hand, the centralized collection of transaction data would pose risks related to privacy and security. Thus, the Reserve Bank of India, is considering hybrid CBDC architecture where some layers of the CBDC technology stack could be on the centralised system and the remaining be on distributed networks (RBI 2022).

11.5. Concluding Observations

The burgeoning digitisation has revolutionised the Indian banking system, but has also brought many cyber security related challenges. In order to stay ahead in the era of dynamic threat landscape, banks need to adopt emerging technologies such as Artificial Intelligence, Machine Learning and Blockchain. This chapter describes the potential of these technologies in the area of cyber security. It highlights the fact that as the traditional security solutions are inadequate to control modern-day attacks, banks can deploy ML based tools to detect and control such attacks. Supervised ML models use the past events data, where machines can be trained to predict definite outcomes (such as identifying Spam,Phishing email, etc.). However, as attacks are evolving everyday, banks may find it difficult to explicitly describe or 'label' such events where unsupervised learning methods would help them form the groups of normal behaviour of systems and spot the abnormility, if any.

The chapter also explains how blockchain technology can provide several opportunities in building next generation security applications. By constructing extremely robust and reliable records of events, it will allow information sharing by creating networks controlled by none, but verifiable and trusted by everyone. The key feature of decentralisation in blockchain overcomes the problem of single target getting compromised to infiltrate and corrupt entire systems and hence blockchain may be one of the most efficient technologies for mitigating cyber risks in the days to come.

However, these technologies can also be potentially exploited by miscreants. A smart hacker may launch an attack on organisation using ML techniques or he/she may exploit some loophole surrounding blockchain system. As cryptocurrency is the most popular application of blockchain, the discussion on blockchain-attacks always revolves around crypto heists. However, the possibility of similar attacks on other blockchain applications cannot be ruled out. Hence, banks need to remain vigilant when they deploy blockchain in areas like trade finance, cross border remittance, etc. Though it is extremely difficult to hack the core application, there may be weaknesses outside the blockchain that create opportunities for attackers and hence banks cannot afford to have false sense of security just because they are using blockchain based applications.

Thus, banks, in their cyber risk management framework need to include guidelines for early identification and handling of risks in adopting emerging technologies. A risk-based approach would help banks in deciding proper controls in early stage of adoption of AI or blockchain and ensure that these technologies are successfully integrated into the business.

References

Arulkumaran K, Deisenrot M P and Brundage MandBharath A A (2017). "A Brief Survey of Deep Reinforcement Learning", *arXiv:1708.05866v2*

Aamir M and Zaidi S (2021). "Clustering based semi-supervised machine learning for DDoS attack classification", *Journal of KS University - CIS,* 33(4), pp.436-446.

AlavizadehHand Jaccard J J (2021). "Deep Q-Learning based Reinforcement Learning Approach for Network Intrusion Detection", *arXiv:2111.13978*

Ayo I, Williams T, Adebiyi and Alagbe O (2021). "An implementation of real-time detection of cross-site scripting attacks on cloud-based web applications using deep learning", *Bulletin of Electrical Engineering and Informatics*, 10, pp.2442-2453

Bhasin, Ramsdell E, Alva A, Sreedhar R and Bhadkamkar M (2018). "Data Center Application Security: Lateral Movement Detection of Malware using Behavioral Models, *SMU Data Science Review*: 1(2).

Bruno G (2016). *https://www.nytimes.com/2016/08/13/business/dealbook/bitcoin-blockchain-banking-finance .html*

Buber E, Diri B and Sahingoz O (2018). "NLP Based Phishing Attack Detection from URLs". *10.1007/978-3-319-76348-4_59.*

Chandrasekar R and Manoharan R (2012). "Malware Detection using Windows API Sequence and Machine Learning", *International Journal of Computer Applications*. 43. 12-16. 10.5120/6194-8715.

Chunfen B (2018). "Network Security Based on K-Means Clustering Algorithm in Data", SNCE Conference Mining Research

Cimpanu C (2018). "IOTA Cryptocurrency Users Lose $4 Million in Clever Phishing Attack", *https://www.bleepingcomputer.com/news/security/iota-cryptocurrency-users-lose-4-million-in-clever-phishing-attack/*

Dada E J, Bassi J S, Chiroma S, Abdulhamid S M, Adetunmbi A O and Ajibuwa O (2019). "Machine learning for email spam filtering: review, approaches and open research problems," Heliyon,Elsevier

Das, S (2022). *https://www.livemint.com/news/india/40-of-global-real-time-payments-originated-in-india-in-2021-report-11650973119569.html*

Datta A (2021). "Detecting phishing websites using machine learning technique", *https://doi.org/10.1371/journal.pone.0258361*

etherchain_org, (2020). *https://twitter.com/etherchain_org/status/1299822510607917056*

Forescey D, Bateman J, Beecroft N and Woods B (2022), "Systemic Cyber Risk: A Primer", *https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer- pub-86531*

Guo Y (2023). "A review of Machine Learning-based zero-day attack detection: Challenges and future directions", *Computer Communications*, 198, pp.175-185

Hindy H , Atkinson R , Tachtatzis C and Colin J (2020). "Towards an Effective Zero-Day Attack Detection Using Outlier-Based Deep Learning Techniques", *https://www.researchgate.net/publication/342547945_Towards_an_Effective_Zero-Day_Attack_Detection_Using_Outlier-Based_Deep_Learning_Techniques*

Hisham G (2015). "Behavior-based features model for malware detection". *Journal of Computer Virology and Hacking Techniques*. 12. 10.1007/s11416-015-0244-0.

Ileberi, E, Sunand Y and Wang, Z. (2022). "A machine learning based credit card fraud detection using the GA algorithm for feature selection". *J Big Data 9, 24. https://doi.org/10.1186/s40537-022-00573-8*

Jagannathan J and Mohamed P (2022). "Security breach prediction using Artificial Neural Networks", *Measurement: Sensors*, 24

Kumari, K and Mrunalini M (2022). "Detecting Denial of Service attacks using machine learning algorithms". *J Big Data 9, 56. https://doi.org/10.1186/s40537-022-00616-0*

Lah A, Dziyauddin R and Azmi M (2018). "Proposed Framework for Network Lateral Movement Detection Based On User Risk Scoring in SIEM. 149-154. *10.1109/TAFGEN.2018.8580484*.

Lim E, Tan G, Hock T and Lee T (2020). "Hacking Humans with AI as a Service", *https://media.defcon.org/*

M. Shashanka, Shen M and Wang J (2016). "User and entity behavior analytics for enterprise security, 2016 IEEE International Conference on Big Data (Big Data)", pp. 1867-1874, *doi: 10.1109/BigData.2016.7840805.*

Muralidharan T and Nissim N (2023). "Improving malicious email detection through novel designated deep-learning architectures utilizing entire email", *Neural Networks*, 157, pp.257-279.

Munene V (2022). "Top 7 Blockchain Domain Name Services (DNS) to Try Out in 2022", *https://blockzeit.com/top-7-blockchain-domain-name-services-dns-to-try-out-in-2022/*

NIST (undated): *https://csrc.nist.gov/glossary/term/threat_intelligence*

Ohri N (2022). "Private banks reported most data breaches in 2018-22: Parliament told", *https://www.business-standard.com/article/companies/private-banks-reported-most-data-breaches-in-*

2018-22-parliament-told-122080201419_1.html

Palmer D (2020). "Major Crypto Exchanges Bitfinex and OKEx Hit by Service Denial Attacks", *https://www.coindesk.com/markets/2020/02/28/major-crypto-exchanges-bitfinex-and-okex-hit-by-service-denial-attacks*

RBI (2020). "RBI Bulletin, Feb, VOLUME LXXIV NUMBER 2", *https://rbidocs.rbi.org.in/rdocs/Bulletin/PDFs/0BUL11022020FL847E8EFB3474 4BAE BB2E45E91759ACCD.PDF*

RBI (2022). "Concept Note on CBDC", Oct, *https://rbidocs.rbi.org.in/rdocs/PublicationReport/ Pdfs/ CONCEPTNO TEACB531172E0B4DFC9A6E 506C2C24FFB6.PDF*

Rudd E, Harang R and Saxe J (2018). "MEADE: Towards a Malicious Email Attachment Detection Engine", *arXiv:1804.08162*

S. Lakshminarasimman, S. Ruswin and K. Sundarakantham (2017). "Detecting DDoS attacks using decision tree algorithm", *Fourth International Conference on Signal Processing, Communication and Networking (ICSCN), 2017, pp. 1-6, doi: 10.1109/ICSCN.2017.8085703.*

Shaheed A and Kurdy M (2022). "Web Application Firewall Using Machine Learning and Features Engineering, Security and Communication Networks", *https://doi.org/10.1155/2022/5280158*

Sur A (2022). "Ransomware attacks in India log in 51% spike in first half of FY22: CERT-In", *https://www.moneycontrol.com/news/business/ransomware-attacks-in-india-log-in-51-spike-in-first-half-of-fy22-cert-in-8943891.html*

Techdesk (2022). *https://indianexpress.com/article/technology/crypto/the-return-of-the-sharkbot-malware-heres-how-to-protect-yourself-8133847/*

Tsihitas T (2022). *https://www.comparitech.com/crypto/biggest-cryptocurrency-heists*

Vishnu B and Jevitha Kp (2014). "Prediction of Cross-Site Scripting Attack Using Machine Learning Algorithms". *1-5. 10.1145/2660859.2660969*.

Wang J (2017). *https://www.databricks.com/session/deep-learning-in-security-an-empirical-example-in-user-and-entity-behavior-analytics-ueba*

Weston, G (2002). Blockchain-impact-on-digital-identity.

URL: https://101blockchains.com/blockchain-impact-on-digital-identity/