

# Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems

Iffath Tanjim Moon<sup>1</sup>, Muhammad Shamsuzzaman<sup>1</sup>, Muhammad Musfiqur Rahman Mridha<sup>1</sup>,  
Abu Sayed Md. Mostafizur Rahaman<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, Begum Rokey University, Rangpur, Bangladesh

<sup>2</sup>Department of Computer Science and Engineering, Jahangirnagar University, Dhaka, Bangladesh

Email: iffathtanjim2197@gmail.com, szaman@brur.ac.bd, mdmridha100730@gmail.com, asmmr@juniv.edu

**How to cite this paper:** Moon, I.T., Shamsuzzaman, M., Mridha, M.M.R. and Rahaman, A.S.M.M. (2022) Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems. *Journal of Computer and Communications*, **10**, 103-129.

<https://doi.org/10.4236/jcc.2022.107007>

**Received:** June 14, 2022

**Accepted:** July 26, 2022

**Published:** July 29, 2022

Copyright © 2022 by author(s) and Scientific Research Publishing Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## Abstract

In recent decades, day-to-day lifestyle requires online payments as easy and simple solutions to several financial transactions, which makes the concept of Electronic payment Systems very popular in the growth of a cashless society. In fact, cashless transactions through simple mobile apps are not merely a concept anymore rather are implemented robustly and being used extensively. On the dark side, obvious financial benefits are making these apps vulnerable to being attacked, which can be successful through security breaches. These cybersecurity issues need to be traced out and resolved to make the financial transactions through an app secure and trustworthy. In this paper, several related papers are analyzed to trace out possible cybersecurity issues in the domain of Electronic Transaction System. The objective is to establish sufficient theoretical background to propose methodologies for measuring security issues and also identify the security strength of any FinTech application and provide standard security metrics.

## Keywords

Fintech Apps, Cybersecurity, Cashless Transaction, Mobile Banking, Electronic Payment

## 1. Introduction

The development of internet resources and services is empowered by the extensive progress of mobile phone technology. The technology of the mobile phone, especially the smartphone, makes the conduction of several tasks extremely easy,

even making a substitution for computers. In fact, the current smartphones are mini-computers that are capable of performing almost all the tasks that a general computer can do [1]. Hence, the usage of smartphones among the masses of people is increasing exponentially. Because of the growth of smartphone users, a large number of monetary organizations are expanding their investment in the development of mobile applications. The goal is to reach those clients who have access to only a smartphone, or at least to a basic mobile phone. That is, an endeavor (successful, however) to cover people of all classes, from rich to poor and from educated to uneducated. As a result, a significant expansion of mobile payment systems is witnessed. A Fintech app or mobile payment application permits clients to accomplish transactions with mobile phones in real-time from anywhere. So, the people do not need to go to the bank or the respective financial organization for any type of transaction. All he/she needs is to have a smartphone or simply a mobile phone, and that can be sufficient to do anything. This brings about a lot of benefits saving time and money and making services available to marginal people and people from inaccessible places. However, the advancement in the usage of these apps has also issued an increased number of vulnerabilities which ultimately directs the apps to cyber-attacks. In fact, this expansion of the cyber world is expanding the attack surface of cyber attackers as well as cybercriminals. Importantly, when the app or electronic system is financial, it creates intense interest among the cyber attackers and cyber criminals to place an attempt considering immense financial advantage. And it is a matter of fear that a significant number of these cyberattacks are successful nowadays [2] [3]. As a result, monetary organizations, as well as clients, are harmed financially. Hence, a terrible threat to the whole financial world that can commit an irretrievable loss to the organizations as well as to the clients. So, in the current situation, the most important concern of these apps is privacy and security which should be considered and ensured before it is too late.

Some numerical measurements can be provided to perceive the current state of affairs as well as the future possibilities of Fintech apps. In the United States, \$5.44 trillion was the transaction value of the digital payments market in 2020, and recent statistics propose the projection to be worth \$11.29 trillion in 2026 [4]. In Canada, it is the amount of \$5.1 trillion worth the total electronic transfers in 2020 [5]. In Singapore, the total transaction value only for the segment of digital payments is predicted to hit around \$17 billion by the end of the year 2022 [6]. Whereas in Pakistan, the transaction value is assumed to outreach around \$6.0 billion by the end of the current year (2022) for the segment of digital payments [7]. In India, the amount is around \$300 billion which is the value of digital payments in the financial year 2021. However, it is projected to be \$1.0 trillion by the financial year 2026 [8]. According to the central bank of Bangladesh, in November 2021, the total amount of digital transactions was \$7905.37 [9]. So, it is apparent that digital payments and transactions are wide-spreading extensively worldwide. That in turn, increases the necessity for robust, secure and trustwor-

thy Fintech apps. Hence, the Security Measures (SM) of a financial app is required to be specified. It's important for developers, as well as clients, to be acknowledged the cybersecurity issues of mobile payment applications.

This paper addresses the most recent security threats, cyberattacks, and vulnerabilities in using Fintech apps and, for this purpose, reviewed a list of articles from various reliable sources and renowned journals. Several possible recommendations and solutions are figured out to cope with the cybersecurity issues and classified the security parameters.

The entire paper is divided into a total of nine sections for ease of following and understanding, including the current one as the introduction to the paper. In Section 2, the related articles are reviewed. The fundamental concepts and components are discussed in the 3<sup>rd</sup> section. In Sections 4 and 5, the current security issues and most occurring cyberattacks are discussed respectively. In Section 6, the technologies for cybersecurity and security environments are discussed. In Section 7, some security requirements for mobile banking apps are described. Sections 8 and 9 are dedicated to the description of learning outcomes, future works and conclusions.

## 2. Previous Works

Cybersecurity concerns are one of the most interesting research fields for experts and researchers nowadays because of their prominent necessity. However, a proper subset, the cybersecurity aspects for the Fintech apps, is creating more interest among the experts because of being the first-choice targets of the cyber attackers. One fact can be mentionable to understand the total contribution workload in this sub-field: the cyber attackers do not consider the cyberattacks as attacks but rather an investment of time and money for some financial benefit [10]. A deep study of hands-on works, studies and papers that are closely related to the scope of this paper is provided. It is divided into three sub-sections to discuss the related works according to the related sub-domain.

### 2.1. E-Wallets and Mobile Payment System

Wodo *et al.* elucidated salient elements of the security system on electronic and mobile banking, covering the technical areas as well as areas related to user awareness and consciousness. Burning issues and solutions like reliable password patterns, proper system software maintenance, secure network selection, biometrics solutions, sandbox mechanism against forceful transactions, two-factor authentication, two-level implementation of security: for non-operational and operational activities, vulnerabilities of SMS codes, phishing based social engineering attacks and preventions are discussed in detail. Numerous authentication mechanisms, legislative improvements, and protection against unauthorized access and theft of data are proposed [11].

Bosamia *et al.* proposed a threat model with all its integral parts discussed in depth considering possible threats on principle components of mobile applica-

tions specific to E-wallets. Also, a comparative analysis of the used technologies and interfaces in numerous E-wallet applications is provided [12].

Bhatnagar *et al.* analyzed the data security issues of mobile banking applications in the context of Inter-Process Communication (IPC), Inter-Component Communication (ICC), and an Application Programming Interface (API) in the android operating system. A research methodology is provided to investigate the activities of the intents (messaging objects used in IPC or ICC) with fuzzing techniques to find out possible data leaks considering the Mobile Application Security Vetting Standard (MASVS) of OWASP as standard. Fuzzing techniques of Mutation and Generation which are provided by various tools with the enhanced facilities to be customized are applied. Security weaknesses relating to architecture, data leaks, malevolent intent activities, and unhandled and inappropriately handled exceptions were found as the result of the methodology [13].

Singh *et al.* conducted a comparative cybersecurity analysis on several digital wallets considering authentication, confidentiality, integrity, availability, and accountability as a few security objectives. Also, remarkable vulnerabilities and threats including attack surface enlargement, insecure APIs, malicious insiders, buffer overflows, vulnerabilities of platforms, social engineering, malicious code insertion, unlawful access, biometric system hacks, SIM card and smartphone cloning, etc. are discussed that may have drastic impacts on the defined security objectives [14].

Ahmed *et al.* discussed different security models of mobile phones and considerable mobile payment systems with their exploit technologies: near field communication, QR-code, radio frequency identification, Bluetooth, SMS, the universal second factor, and payment procedure with their security mechanisms. Various parameters of mobile payment systems are exposed where socioeconomic circumstances, diffusion of mobile phones, cost-efficiency, convenience, security issues, underdeveloped ecosystem, restrictions, and collaboration are considered. The mobile payment system with its key attributes is described where authentication, confidentiality, access control, integrity, availability, and non-repudiation is focused. The encryption technology of mobile payment systems involves symmetric key encryption, where an identical key is employed to encrypt and public-key encryption, where two distinct keys (public, private) are used. Several types of cyber attacks on mobile payment systems are stipulated specifically, obtaining the PIN of the user, brute force attacks of PIN, attacking MMS traffic and server, etc. [15].

## **2.2. Mobile Application and Computing Context**

Botas *et al.* proposed a three-phased methodology to inspect mobile applications in order to discover and analyze cybersecurity issues like malevolent behaviors, possible vulnerabilities, coding level issues, faulty designs that can be subjected to detrimental, etc. The first phase is composed of analyzing components from reverse engineering in depth and investigating information gatherings by the

application. The second one consisted of analysis of the activities during the running of the application like handling and accessing of data and files including sensitive ones, the behavior of networks, and the execution of the source codes, etc. The last one consists of the analysis of modules that were subjected to be changed during the running of the applications like internal database, downloaded files, and internal storage of credentials: keychain, cookies, logs of execution files, etc. However, the methodology depends on some analysis blocks consisting of the top ten risks in the Open Web Application Security Project (OWASP, 2014) [16].

Sarker *et al.* proposed a general-purpose multi-layered framework implementing advanced machine learning techniques to develop automated and intelligent cybersecurity systems where heterogeneous security data were analyzed. In fact, cybersecurity modeling is proposed to be developed based on machine learning with security big data analytics. Basically, in this paper, cybersecurity data science is discussed to reveal how intelligent and actionable the computing process can be to ensure cybersecurity [17].

In another paper, Sarker *et al.* exposed cybersecurity intelligence, automated and, at the same time, smart modeling to manage cybersecurity issues in an intelligent manner where various artificial intelligence (AI) approaches like machine learning (ML) enhanced by deep learning, natural language processing (NLP), knowledge representation and reasoning (KRR), rule-based expert systems (RBES) are implemented. Malware detection and analysis, malevolent behavior detection, phishing attack identification, malicious code detection, etc., can be carried out with this modeling based on AI. In fact, cybersecurity analysis driven by AI is the main focus of this paper [18].

### 2.3. Techniques and Mechanism

Asher *et al.* proposed a methodology to analyze reverse engineering tools on the applications specific to mobile banking from the systematically collected and sorted dataset. Shrewd enough research questions were defined and answered considering the criteria of time complexity, generation of errors, and the number of resulting files. Observations of the analysis can be listed: a time-consuming procedural creation of decompiled APK files in an obfuscated form, filing the error details in text format, and creation of many files from one APK file. However, the outcomes were not identical for different tools. It is worth to be mentioned that comprehensive reverse engineering was not under the capability of a single tool [19].

The literature reviewed in this section conforms to the specified subject and is important enough to be mentioned before going to the next sections. However, the first sub-section is the most-close of the Fintech apps, but the later ones are also explained as they are important as well.

## 3. Key Concepts and Technologies

Diving deep into the cybersecurity aspects requires adequate knowledge about

the technological and conceptual components that are related to the specified domain. This section serves that purpose. Multidisciplinary aspects with emphasis on technical terms are considered.

### **3.1. E-Wallet/Digital Wallet**

An E-wallet can be introduced as a tool, software application, or program that collects identity authenticity information with the information of financial cards or bank accounts and offers real-time services to perform specified financial transactions online through electronic devices like mobile phones, computers, etc. [20] [21] [22] [23]. Even offline transactions can be made through some E-wallets, namely, bKash (Brac Bank), Rocket (Dutch Bangla Bank Limited), etc. with basic mobile devices using a USSD interface where minimal cellular functionalities are available [24] [25]. Experts of different, even similar fields named it differently, for example, digital wallet, m-wallet or mobile wallet, cyberwallet (obsolete), etc. although the concepts are almost the same. To carry and use several financial or payment cards like debit cards, credit cards, gift cards, prepaid cards, etc., in a virtual manner for performing financial transactions is made possible by E-wallet which is creating a significant possibility for the elimination of physical wallets [21]. Some E-wallets provide facilities for putting amounts equal to cash of a certain limit in accounts that can be done from their respective easily available agents for cashless transactions [24] [25] [26]. Nowadays, several E-wallets are in massive use in international as well as national domains due to being adaptive, easy to use, convenient, fast and secure [23]. There are a few terms and concepts solely related to the concept of E-wallet are also introduced.

### **3.2. Cashless Transactions**

Cashless transactions can be defined as such financial transactions among the respective parties where banknotes or coins are transacted as digital information or digital currency or in the form of electrical representation of cash instead of the physical form. As a payment method, digital payment via transacting digital agreed-upon entities is prioritized over cash payment in cashless transactions [27]. In fact, it's a solution to payments without physical cash, an entry to the future cashless economy where goods and services are available in exchange for electronic payments [28]. Although the term cashless transaction was coined years before the term E-wallet, it is being promoted by E-wallet and is being used as a strong medium these days.

### **3.3. Payment Cards**

Payment cards are financial cards that authorize the card possessor with the right to access as well as performing transactional operations of electronic funds and allowing ATMs access, fastened with financial accounts like bank accounts, credit accounts, etc. Financial institutions issue payment cards including ATM cards, credit cards, debit cards, charged cards, gift cards, prepaid cards, etc. [29].

Security is enhanced by adopting the technological innovations of Magnetic Stripes (Magstripe), EMV chips, Near Field Communication (NFC), APIs, etc. [30].

### **3.4. Mobile Banking**

The concept of mobile banking or m-banking is a blessing of mobile technologies as well as mobile internet in the financial sector, which can be presented as an implementation of mobile commerce authorized by financial institutions like banks to carry out financial operations or transactions, avoiding direct interactions with banks even ATMs [31] [32] [33] [34]. Remote payments, money transfers, Management of financial accounts like bank accounts, participation in the stock market by buying and selling stocks and so on could be the available financial services [33]. These services can be relished by permission through dedicated mobile banking applications, short message services (SMS), mobile calls, etc., using devices like Personal Digital Assistants (PDA), smartphones and even basic mobile phones for accessing banking networks [31] [34].

### **3.5. E-Banking**

E-banking can be defined as a process where a client can interconnect digitally with a bank using a computer, laptop or a kiosk to perform several financial or banking activities without any human intervention [31] [35]. These activities include transactions of funds, ordering new cheque books, online payments of bills, requesting bank statements, investing in the stock market and management of account savings and fixed deposits, paying insurance installments, etc. There are similar suitable phrases namely, Online Banking, Electronic Banking, Internet banking, etc. that are used in the same sense [35].

### **3.6. Digital Currency**

Digital currency, also called e-cash, can be defined as a format of currency that is digital and that is equivalent in amount to fiat currency for any financial transaction. The central authorizer of a physical currency is also the authorizer of the equivalent digital currency and has control over the monetary value [36] [37]. In E-wallet or Mobile banking-based applications or software and in ATMs, it is used as currency for various financial operations instead of physical cash. There is another type of currency named cryptocurrency, which is sometimes considered a digital currency and is beyond the discussion of this paper.

The entire system of electronic payment system and the functionality of the Fintech apps can be illustrated with the concepts of these fundamental components. Also, this discussion creates a strong base for further deep invasion.

## **4. Security Issues**

In recent years, the considerable recognized payment technique in equally rising economies and current society, the mobile payment application or e-wallet, has

been significantly famous. As a result, the cyber security issues of mobile payment applications to defend the cyber-threats are a major apprehension of the software developer and user. A group of technologies and methods schemed to defend computers, software, networks, and data from being impaired by various types of cyberattacks or unauthorized entrance are comprehended as Cybersecurity [17]. On the other side, a malevolent and premeditated endeavor by a person or system to access forcefully the information of any computerized process of another person or system is termed a cyberattack. Typically, some sort of advantage by hampering the privacy of the sufferer's information using the unauthorized entry is aimed by the attacker [38].

Open Web Application software (OWASP) is a Foundation that updates the security metrics for web application developers as well as e-payment system developers [39]. We have addressed the OWASP identified critical security issues in **Figure 1**, along with some more unavoidable threats in **Table 1**.

A mobile payment application must include the objectives—Authentication, Integrity, Availability, Confidentiality and Accountability to assure cybersecurity [14]. A mobile payment application or e-wallet becomes vulnerable when several types of cyberattacks are committed against these main objectives. The security of a system, person, susceptible data, or network is engendered by different kinds of cybersecurity affairs, which are demonstrated in **Table 1**. [17] [40]-[52]. Security issues are most vulnerable to attacks, which is represented in brief in **Table 1** below. The detailed **Table A1** is in Annex.

## 5. Cyberattacks on Electronic Payment System







The financial benefit is the primary goal of attacking an electronic payment system or application by hackers. The scope of attacks is sectioned into three major



**Figure 1.** OWASP Top 10 [39].



**Table 1.** Cybersecurity affairs.

Cybersecurity	Interpretation	Instance
 <b>Phishing</b>	<ul style="list-style-type: none"> <li>• A state of social engineering</li> <li>• Spurious endeavor to acquire tactful information including login data, credit card info, and so on</li> <li>• Using email, messages as a medium</li> </ul>	<ul style="list-style-type: none"> <li>❖ An attack of spear-phishing against Twitter personnel accessing the account of some celebrity</li> </ul>
 <b>Malware</b>	<ul style="list-style-type: none"> <li>• One sort of malicious software</li> <li>• Allowing unauthorized entrance to the server, computer, network, etc.</li> <li>• malware comprising worms, adware, viruses, spyware, Trojan horses, ransomware, malicious bots, and so on</li> </ul>	<ul style="list-style-type: none"> <li>❖ A ransomware attack upon the health service of Ireland blocked the employees away from their associated computer systems</li> </ul>
 <b>DDoS attacks</b>	<ul style="list-style-type: none"> <li>• An attack aimed by zombies, bots</li> <li>• An endeavor to collapse a server, network, machine by encumbering it through traffic</li> <li>• through the medium of the simple network management protocol (SNMP)</li> </ul>	<ul style="list-style-type: none"> <li>❖ Distributed denial of service (DDoS) attacks emerged on numerous websites of banks and departments of the government of Ukraine</li> </ul>
 <b>Man In the Middle</b>	<ul style="list-style-type: none"> <li>• An attack of eavesdropping</li> <li>• It's seemed to be a usual interaction of information by eavesdropping or simulating devices</li> <li>• Injection of false data and commands are performed by the introducer</li> </ul>	<ul style="list-style-type: none"> <li>❖ The warning of the vulnerability of eavesdropping is reported for the numerous famous website</li> </ul>
 <b>Injection</b>	<ul style="list-style-type: none"> <li>• Injection of malevolent code inside the application for obtaining the data of the user</li> <li>• The concatenation of Hostile data is exploited</li> <li>• SQL, Object Relational Mapping, NoSQL, LDAP, OS command, Object Graph Navigation Library injection are usually familiar injections</li> </ul>	<ul style="list-style-type: none"> <li>❖ Through the SQL injection, around 5 million clients' databases of Vtech were hacked</li> </ul>
 <b>Zero-Day Attack</b>	<ul style="list-style-type: none"> <li>• Unknown susceptibility of any system which is concerned to manipulate with malevolent actions</li> <li>• Until architects determine the blunders, the exposures could be continued over days or a few months, even years</li> <li>• Without awareness of the security, the software version is released</li> </ul>	<ul style="list-style-type: none"> <li>❖ The zero-day attacks emerged on the File Transfer Appliance (FTA) of Accellion. The confidential data owned by the clients were embezzled through the attacker</li> </ul>

categories by which an anonymous unwanted user can get exact information to breach the security of a Fintech App. However, these three major categories are part of a proper subset of the five essential categories mentioned in the previous section as objectives [14]. They are covered considering their explicit importance in cybersecurity.

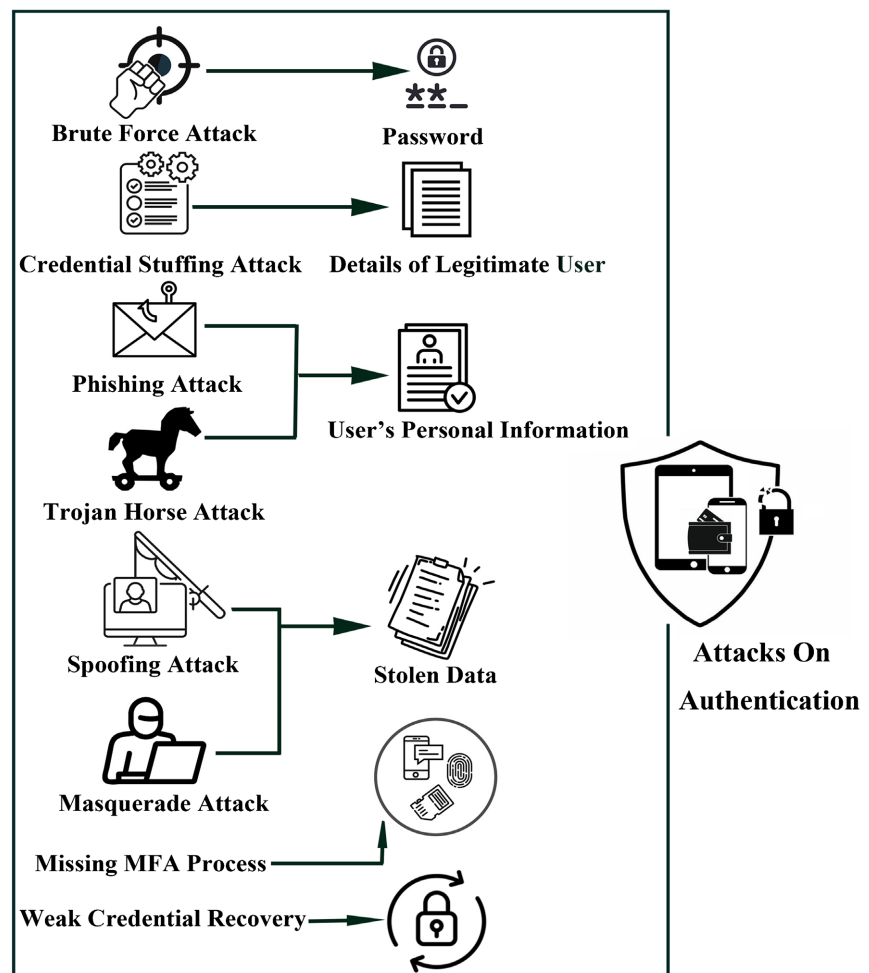
### 5.1. Attacks on Authentication

Multifarious attacks are consummated on diverse pivotal access information to breach the authentication method of an E-Wallet. Violating the authentication through the brute force attack, which is performed on the password of the

E-Wallet [15] [50]. The vulnerable authentications system allows credentials stuffing attacks by an intruder who is well-informed with the details of the legitimate users including the name of the user, password, and so on. Phishing attack, as well as Trojan horse attack, attempts to snatch tactically the personal information of the users like login data, and credit card information. Spoofing attack and also masquerade attack is performed by stealing several types of user data. As a result of these attacks, the authentication becomes a failure by giving unauthorized entrance into the E-wallet. In addition, the absence of multifactor authentication and poor credential recovery system makes the authentication to be way more vulnerable. The attacks and vulnerability for the authentication of an E-Wallet are illustrated in **Figure 2**.

## 5.2. Attacks on Integrity

Another major care of an Electronic Payment System is Integrity, concerning the immutability of users' information. If the information is entranced and mutated by the attacker, the integrity of the E-Wallet is endangered [15]. In a salami attack, archenemies are authorized to withdraw money through the process of

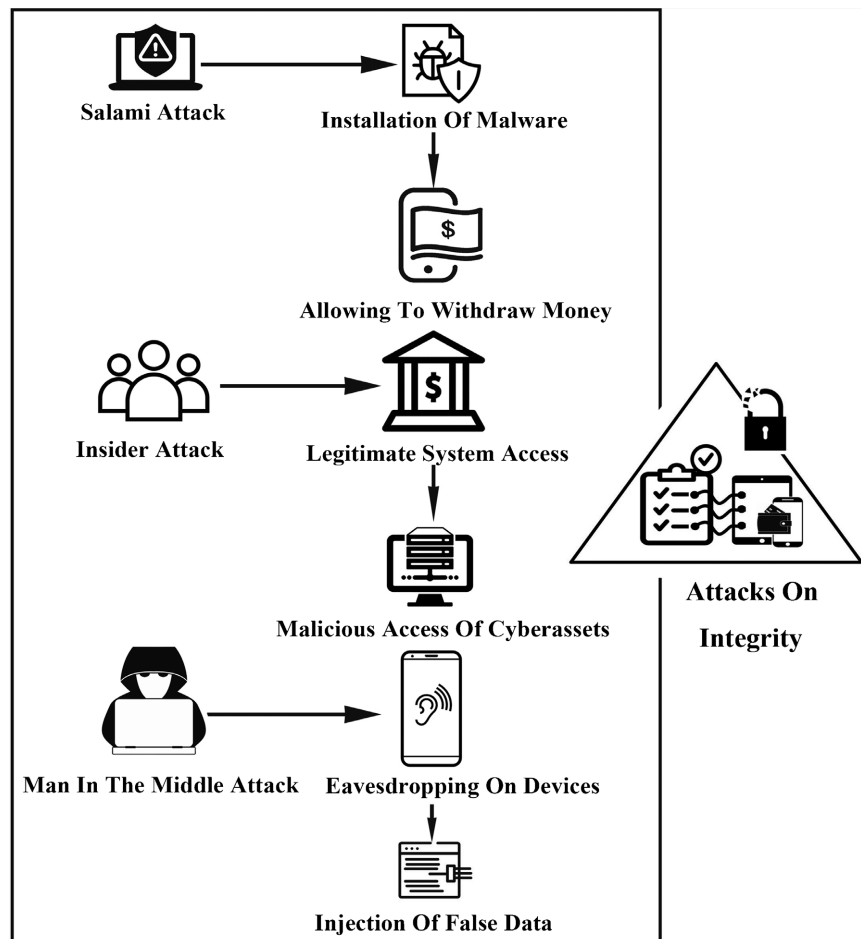


**Figure 2.** Attacks on authentication.

installation of malware into the server [53]. As the insiders are permitted to penetrate the cyber assets of the system, hence an adequate possibility is to be impaired the integrity of data by the malicious insider compared with an exterior invader [54]. In Man in the Middle attack, through eavesdropping on communication, the attacker impersonates an authorized user to mutilate the information or inject fraudulent data for exploiting the transactions in real-time, the transmission of data, and so forth [15] [55]. In consequence, these illegitimate mutations and annihilation of information and also unobserved modifications violate the integrity of an E-Wallet. The attacks and vulnerability to the integrity of an E-Wallet are illustrated in **Figure 3**.

### 5.3. Attacks on Availability

The deliberate discontinuation of the server of the E-Wallet application by a rival is considered an attack on availability. Distributed denial of service (DDoS) attack is one of the greatest accusations in cyber security. In a DDoS attack, the attacker blocks the permissible traffic by transmitting fraudulent traffic [15]. At once, the DDoS attack can down the server for many hours by hacking together hundreds or thousands of devices. Comparatively, the Denial of service (DoS) is



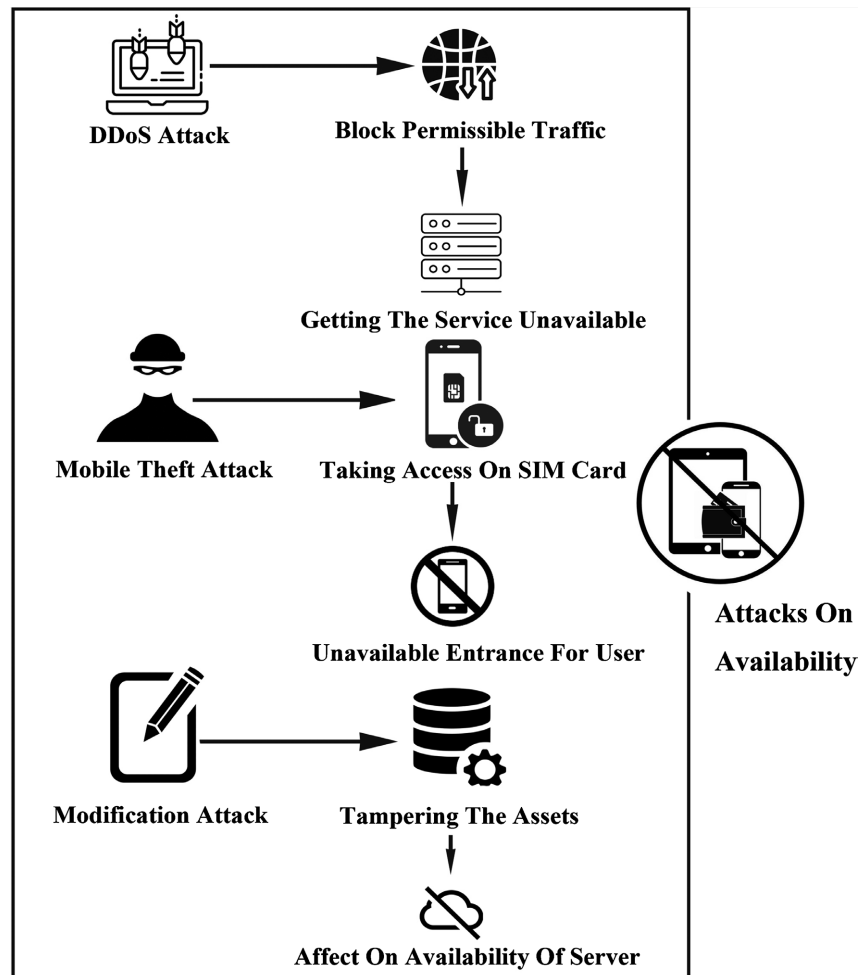
**Figure 3.** Attacks on integrity.

deemed a specific attack on a single device [56]. After a DDoS attack, the services of an authorized user get unavailable. In a mobile theft attack, the SIM card of the stolen mobile is accessed by the attacker. As a consequence, it eventuates the unavailability to access legitimate users into E-Wallet. By tampering with the resources, the modification attack affects on availability of the server. The attacks and vulnerability of the Availability of an E-Wallet are illustrated in **Figure 4**.

The various cyberattacks and various aspects of cyberattacks, including Attacks on Authentication, Attacks on Integrity and Attacks on Availability are illustrated with adequate explanation. These cyber-attacks are needed to be defined to recommend technological tool kits, instruments and systematic procedures and approaches.

### 6. Communicating Environment and Technologies

There are a lot of tools, technologies and solutions for communication, payment, authentication and security that are currently being used in Electronic Payment Systems. These are being used to make the features and financial transactions to



**Figure 4.** Attacks on availability.

be performed offered by E-wallets more secure, convenient, and extensive.

### 6.1. Near Field Communication (NFC)

Near Field Communication (NFC) can be defined as a set of standards or protocols of radio transmission that offers opportunities for transmitting or interchanging data in short-range around 0.04 to 0.1 meters (sometimes can range up to 0.2 meters) within two devices, electronic as well as digital, with half-duplex mode [57] [58] [59] [60]. Hence, the communicating devices must be near enough or attached physically for a successful data transmission phase and the measurement of proximity depends on the radiated power of the used antenna [58]. In this radio communication technology, radiofrequency (RF) signals are used for the transferring of data, with a low operating frequency that equals 13.56 MHz and inductive coupling is implemented [57] [61]. However, NFC requires low power providing a minor data transmission rate, measurably around 0.424 Mbps, whereas another wireless technology, Bluetooth 5.2 has a data transmission rate of around 50 Mbps with a data transmission range of 400 meters [60] [61] [62]. For implementing an NFC system, any of the three operating modes, namely, Peer-to-Peer mode: exchange of data within two NFC devices in an improvised manner, NFC Card Emulation mode: analogous methodology to that of the radio-frequency identification system (RFID) with advanced and enhanced technology, Reader/Writer mode: mode for reading and writing data on NFC chips named tags by NFC devices, can be chosen [57]. It has remarkable utilization in diverse fields, including payment cards like credit cards etc., E-Wallets/Digital Wallets, smart ticketing for transportation systems and events, medical applications or systems that contain smart wireless tags, devices to be worn, sensors etc. [61]. Moreover, the security of E-wallets can be enhanced by NFC as it insists the owner or user move nearer to the shop or payment point, so there is no chance for fraud by remote payments or financial transactions [58].

### 6.2. Quick Response Code (QR Code)

The Quick Response Code, abbreviated as QR Code, is a two-dimensional symbology code or two-dimensional barcode or simply a matrix barcode that can store particular information which can be retrieved when required with a visual scanning tool or technology [63] [64] [65]. In fact, QR Codes are optical labels similar to barcodes that are machine-readable where information is stored in two dimensions: horizontal and vertical and in the form of square or rectangle black dots, named modules, assembled in a perfectly square or rectangular grid on a background color as white [63] [64] [66]. Compared with a conventional barcode, QR codes are cost-efficient and, being quickly responsive makes them time-efficient as well. The two-dimensional layout makes it scannable from 360 degrees with the facility to decrypted data from any angle [64]. QR codes are being used nowadays to encode and store numerous types of information including contact information, physical address information, phone number,

e-mail address, map or geo-location, URL, a particular SMS or text, and access information of a WIFI network, calendar events, etc. [67]. And in the field of E-wallets, since almost all mobiles or smartphones have at least a basic camera that can be used as a QR code scanner and there are huge utilization and future possibilities of QR codes, QR codes are extensively used. However, the practical usage of the QR code reminds the users about the risk and security concerns subjected. The security concerns lie in the dotted code beyond human interpretability with mere eye observation. Bits of codes in a hidden manner can be used to collect user information and malware or phishing attack can be launched with the machine's interpretable code [68]. Fortunately, these limitations can easily be eliminated by proper user consciousness and a well-designed, well-structured, secure-prone and robust QR-code reader [69].

### **6.3. Secure Element (SE)**

A secure element can be defined as a component as an internal part or even an integrated circuit of a hardware device that can be used to provide various security services by resisting any tampering attempt. A long enough list can be developed to mention the services provided by a secure element including detection of tampering attempts, storing the root of any authentication chain, storing and generating of private security keys, services regarding cryptography, secure management of system resources etc. [70] [71]. However, sometimes a secure element is defined by a programmable microcontroller with the construction objective to provide a secure environment for execution and storage. It can be divided into two types broadly: Multos and Java Cards on the basis of underlying Operating System (OS) [72].

### **6.4. HCE (Host Card Emulation)**

Host Card Emulation is basically an advanced cloud technology that makes use of the cloud server to store, access and manage crucial transactional data, dissimilar to an environment (for example, SE) that performs the data management locally in the device. It avails secure contactless payment to be placed in accordance with the NFC technology [73]. HCE technology can be implemented as one of the two HCE NFC models: pure HCE by simulating SE in the way of communicating to a POS terminal without any intervention of a physical SE and hybrid HCE by being associated with the security features of a real security element [74]. This technology should be adopted where rich resources, high performance, excellent user interface, cost efficiency, and high processing speed are expected at the expense of compromised security compared to the technology of that of the SE [75].

The tools and technologies are the most trending and mostly used in the famous and well-known cybersecurity systems and Fintech apps. Hence, the discussed ones can be considered reliable and trusted enough to be used and to be implemented.

## 7. Mobile Banking App Security Requirements

Mobile banking and Fintech app developers must meet the requirements for a secure and trustworthy app. Even financial service organizations want their apps to be protected from fraudulent activities. Developers can follow the security requirements in **Figure 5**, for mobile banking and Fintech apps in developing an app.

### 7.1. Anti-Reverse Engineering

The application developers perform Anti-Debugging and Anti-Tampering to authorize the applications to defend against malevolent reverse engineering. By linking a debugger, the state and execution of the application can be instructed, and then the code can be tempered by attackers [76]. So, the anti-debugging, Android, and iOS anti-reverse engineering shields to the app must be retained these qualities by this shield-like explication. The app from operating simulators and emulators can be inhibited by ensuring this OneShield solution [77].

### 7.2. Code Obfuscation

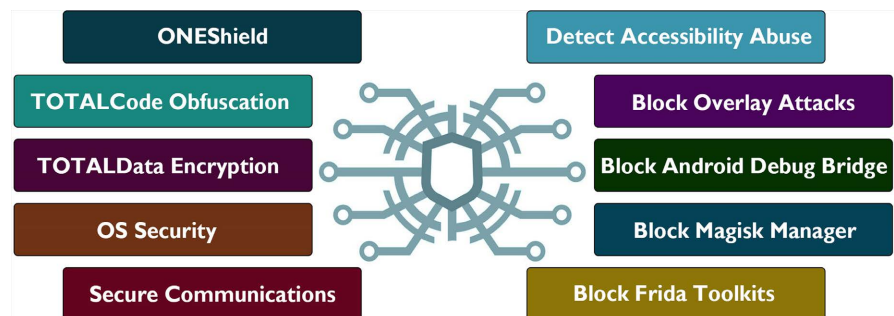
Developers can obfuscate the source code of the application to cover up the entire to confine code tampering and reverse engineering [78]. With SDKs and 3<sup>rd</sup> party libraries, there needs to be the obfuscation of all the components of non-native and binary code [77]. The identifier renaming, control flow obfuscation, string encryption, and reflection obfuscation are comprised of the techniques of Android code obfuscation [79].

### 7.3. Encryption

In the encryption method, to transform plaintext into ciphertext, the encryption algorithm and key are applied while decryption is the opposite method where the decryption algorithm and key are used to bring back the ciphertext into plaintext [80]. In the two-factor authentication of mobile money, the utmost used cryptographic functions are symmetric, asymmetric encryption function, and hash function [81].

### 7.4. Operating System Security

For the shelter of the operating system against attackers, there need to assure the



**Figure 5.** Mobile banking app security requirements [77].

security to obstruct unauthorized alternation of the operating system. A jailbreak is an advanced attack that dispels the prevention of the iOS software to entrance a device and the file system [82]. On the other hand, for the Android operating system, it is known as rooting the device [82]. In the case of banking and Fintech apps, it's significant to make sure Android root prohibition and iOS jailbreak preclusion.

### **7.5. Secure Communications**

In a secure communication mechanism for the network, the data transmissions between the client and server must be protected to defend against unauthorized third-party access. The construction of a protected communication method is mandatory to defend the Man-in-the-Middle (MitM) and further network-arisen threats for any mobile banking and Fintech app. The attacker breaks off and tempers the dispatched data in the Man-in-the-Middle attack, which is extensive in both cyber-physical and computer systems [83]. The invulnerable certificate pinning and bot protection to the apps to additionally shield the connection between the app and the mobile back end is furthermore added by it.

### **7.6. Accessibility Misuse Detection**

The accessibility benefits are intended to assist users with incapability or handicap in guiding their machines [84] [85] [86]. As the current securities do not permit applications to rescue the users with demands of accessibility, the robust functionalities of untrustworthy applications are sometimes misapplied for envious objectives, for instance, the thievery of data from additional apps [84] [87]. Any application ensconced on the device with excessively multiple accessibility assistance authorizations must be tracked out. For all Trojans and RATs, this claim escalation is typical [77].

### **7.7. Prevention of Clickjacking**

Overlay Attack, also known as Clickjacking against user interfaces forms an enigmatic overlay that thoroughly hides a security-tactful application when the user assumes a nonmalignant overlay is interplayed actually on the underneath; the intentional application is interplayed with the user [88] [89]. There must be endured protective actions to defend against overlay attacks on the user interface. Screen overlays attacks, for instance Anubis, StrandHogg, Cloak&Dagger, Ginp, BankBot, Ghimob, BlackRock, and MazarBot from exhibiting a counterfeit screen on the lid of the app screen should be unrolled and forbore [77].

### **7.8. Prevention of Command Line Debugging Tools**

A client-server program like Android Debug Bridge (ADB) acts as a multipurpose command-line tool. With emulator models or linked devices, the users are permitted to transmit data [90]. It enables one in debugging, installing, and troubleshooting Android applications and also supplying Unix shell entrance



[90] [91]. For malevolent reverse engineering and debugging of the application, the usage of ADB needs to be stopped.

### **7.9. Prevention of Rooting Interfaces Misuse**

The rooting interfaces can be introduced as system-less rooting tools, e.g., Magisk Manager, Superuser-ChainsDD, Kingoroot etc., that can provide system-level access to mobiles phone without any altering to the core code, for example, rooting, un-rooting etc. [92] [93] [94] [95]. Unfortunately, these interfaces or tools can also be used for fraudulent activities like illegal rooting, tampering with rooting (root hiding, root cloaking etc.) etc. So, suspicious behaviors and activities must be determined and obstructed to protect against any misuse of these interfaces.

### **7.10. Prevention of Development & Engineering Toolkits Misuse**

There are several toolkits, e.g., Frida, PyREBox, Radare2 etc., that are generally used as a strong instrument for the developers, security experts, security researchers and reverse-engineering experts to do various development and engineering tasks. However, the ill-intentions of the cyber attackers and cyber criminals can lead to the usage of these toolkits for fraudulent activities by injecting malicious codes, extracting private and sensitive data by reverse-engineering, tampering underlying logic of the apps, altering the behavior of the apps etc. [96]-[101]. Hence, the suspicious usage of these toolkits needs to be detected and stopped automatically to avoid any kind of cyberattacks. Strong monitoring and regulating of various activities can help for that purpose [102].

## **8. Learning Outcome and Future Work**

Cashless transaction is a buzzword in today's society and their popularity is increasing day by day. Life becomes easy nowadays with the use of financial technology applications as users can easily do their daily tasks and make transactions with a single finger trip. Within a second, any amount of money transfer is done. In parallel with this security concern with these Apps is a major issue as financial benefit captivates the intruders to manipulate the app data. In our study in this paper, the most recent potential cyber security threats are identified, which creates a question about the reliability of these Fintech apps. Mobile Emulator makes the OS ambiguous to the sole user and the hackers. Moreover, malware drains the app users' data which is also an issue to be taken a look very carefully. Hence, Machine learning algorithms are being used in some cases to cope with the evolved malware. This process of defending against cybersecurity threats is a continuing task with the growth of technology.

In this paper, electronic transactions' potential security threats and attacking modes are studied, but there were limitations in studying the vulnerability assessment matrices with any security model. Future work, therefore, will be to build a security model to identify as well as take protective measures against cy-

ber security threats of these apps. Moreover, a framework for the detection of some particular cyber-attacks based on machine learning will also be another future task so that an AI-enabled automated security model can come into action.

## 9. Conclusions

On the eve of the 5<sup>th</sup> Industrial Revolution (IR 5.0), the expansion of the cyber-world is tending to move society to a cashless one where virtual as well as electronic transactions are becoming more and more universally accepted [103] [104] [105]. This ever-growing popularity of electronic transactions leads financial organizations and agents to the tremendous activities of Fintech app development. However, the features and functionalities are making these Fintech apps stupendous facilities and advantages bringer for the clients, but clean targets for cyber attackers and cybercriminals, on the other hand. Hence, there arises the concern of cybersecurity to protect these apps from cyberattacks and to take care of handling the threats and vulnerabilities. This cybersecurity concern is studied, elaborated, described, and analyzed from some pre-defined aspects throughout this whole paper in a precise and concise manner. The former portion of the paper is dedicated to providing the concepts and components that are related to Fintech apps are explained in a neat and clean manner. Also, an abstraction of related research works and studies is provided collectively that can be very helpful to any further research work or implementation. Naturally, there are some explicit and implicit outcomes and contributions of this paper that can be listed:

- 1) The state-of-the-art cyberattacks, threats, vulnerabilities, cybersecurity issues, and cybersecurity parameters are discovered and analyzed in a concise manner, including Phishing, Malware, DDos attacks, Man in The Middle, Injection, and Zero-Day Attack etc. where the up-to-date real-life instances are considered.

- 2) Some recommendations are provided on the environments, tools and technologies related to cybersecurity, including NFC, QR-Code, HCE, SE, etc. The reason behind this recommendation is their proven trustworthiness and robustness.

- 3) Some cybersecurity requirements are recommended for mobile banking apps, a sub-set of Fintech apps. An abridged keyword-based list could be Anti-Reverse Engineering, Code Obfuscation, Encryption, Security of Operating System and Communication, Detection of Accessibility Misuse, etc. Also, prevention of the phenomenon: Clickjacking, Command Line Debugging Tools, Rooting Interface Misuse, Development and Engineering Toolkits misuse, etc. are also appended. These requirements are of multiple layers and aspects of the apps.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References

- [1] Randazzo, V., Ferretti, J. and Pasero, E. (2020) A Wearable Smart Device to Monitor Multiple Vital Parameters—VITAL ECG. *Electronics*, **9**, 300. <https://doi.org/10.3390/electronics9020300>
- [2] Bunker, G. (2020) Targeted Cyber Attacks: How to Mitigate the Increasing Risk. *Network Security*, **2020**, 17-19. [https://doi.org/10.1016/S1353-4858\(20\)30010-6](https://doi.org/10.1016/S1353-4858(20)30010-6)
- [3] Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M. (2021) Risk Management, Firm Reputation, and the Impact of Successful Cyberattacks on Target Firms. *Journal of Financial Economics*, **139**, 719-749. <https://doi.org/10.1016/j.jfineco.2019.05.019>
- [4] www.businesswire.com (2021) Digital Payments Market Report 2021: Transaction Value Was \$5.44 Trillion in 2020—Global Growth, Trends, COVID-19 Impact, and Forecasts 2021-2026—ResearchAndMarkets.com. <https://www.businesswire.com/news/home/20210604005270/en/Digital-Payments-Market-Report-2021-Transaction-Value-was-5.44-Trillion-in-2020---Global-Growth-Trends-COVID-19-Impact-and-Forecasts-2021-2026---ResearchAndMarkets.com>
- [5] www.fasken.com (n.d.) Payments Canada: Canadian Payment Methods and Trends Report 2021. <https://www.fasken.com/en/knowledge/2021/10/payments-canada-canadian-payment-methods-and-trends-report-2021#:~:text=Electronic%20Transfers&text=In%202020%3A>
- [6] Statista (n.d.) Digital Payments—Singapore|Statista Market Forecast. <https://www.statista.com/outlook/dmo/fintech/digital-payments/singapore>
- [7] Statista (n.d.) Digital Payments—Pakistan|Statista Market Forecast. <https://www.statista.com/outlook/dmo/fintech/digital-payments/pakistan>
- [8] Dec 30, S.C./T.C./U., 2021 and Ist, 12:46 (n.d.) Explained: How India Is Outpacing the World in Digital Payments—Times of India. *The Times of India*. <https://timesofindia.indiatimes.com/business/india-business/explained-how-india-is-outpacing-the-world-in-digital-payments/articleshow/88580555.cms>
- [9] www.bb.org.bd (n.d.) Bangladesh Bank. <https://www.bb.org.bd/en/index.php/financialactivity/mfsdata>
- [10] Huang, K., Siegel, M. and Madnick, S. (2018) Systematically Understanding the Cyber Attack Business: A Survey. *ACM Computing Surveys (CSUR)*, **51**, 1-36. <https://doi.org/10.1145/3199674>
- [11] Wodo, W., Stygar, D. and Błaskiewicz, P. (2021) Security Issues of Electronic and Mobile Banking. *Proceedings of the 18th International Conference on Security and Cryptography—SECRYPT*, Paris, 6-8 July 2021, 631-638. <https://doi.org/10.5220/0010466606310638>
- [12] Bosamia, M.P. and Patel, D. (2017) Wallet Payments Recent Potential Threats and Vulnerabilities with Its Possible Security Measures. *International Journal of Computer Sciences and Engineering*, **7**, 810-817. <https://doi.org/10.26438/ijcse/v7i1.810817>
- [13] Bhatnagar, S., Malik, Y. and Butakov, S. (2018) Analysing Data Security Requirements of Android Mobile Banking Application. In: Traore, I., Woungang, I., Ahmed, S.S. and Malik, Y., Eds., *International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments*, Springer, Cham, 30-37. [https://doi.org/10.1007/978-3-030-03712-3\\_3](https://doi.org/10.1007/978-3-030-03712-3_3)
- [14] Singh, P. and Rajput, R.S. (2019) Cybersecurity Analysis in the Context of Digital

- Wallets. *International Journal of Advanced Studies of Scientific Research*, **4**, 522-525. <https://ssrn.com/abstract=3355789>
- [15] Ahmed, W., Rasool, A., Javed, A.R., Kumar, N., Gadekallu, T.R., Jalil, Z. and Kryvinska, N. (2021) Security in Next Generation Mobile Payment Systems: A Comprehensive Survey. *IEEE Access*, **9**, 115932-115950. <https://doi.org/10.1109/ACCESS.2021.3105450>
- [16] Botas, A., Rodriguez, R.J., Balsa, J., Garcia, J.F., Alonso, J., Lera, F.J., Garcia, C., Matellán, V. and Riesco, R. (2016) Security Assessment Methodology for Mobile Applications. *Spanish National Cybersecurity Research Conference*, Granada, 15-17 June 2016, 50-56.
- [17] Sarker, I.H., Kayes, A.S.M., Badsha, S., Alqahtani, H., Watters, P. and Ng, A. (2020) Cybersecurity Data Science: An Overview from Machine Learning Perspective. *Journal of Big Data*, **7**, 1-29. <https://doi.org/10.1186/s40537-020-00318-5>
- [18] Sarker, I.H., Furhad, M.H. and Nowrozy, R. (2021) Ai-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*, **2**, 1-18. <https://doi.org/10.1007/s42979-021-00557-0>
- [19] Asher, S.W., Jan, S., Tsaramirsis, G., Khan, F.Q., Khalil, A. and Obaidullah, M. (2021) Reverse Engineering of Mobile Banking Applications. *Computer Systems Science and Engineering*, **38**, 265-278. <https://doi.org/10.32604/csse.2021.016787>
- [20] Hassan, M.A., Shukur, Z., Hasan, M.K. and Al-Khaleefa, A.S. (2020) A Review on Electronic Payments Security. *Symmetry*, **12**, 1344. <https://doi.org/10.3390/sym12081344>
- [21] Daragmeh, A., Sági, J. and Zéman, Z. (2021) Continuous Intention to Use e-Wallet in the Context of the Covid-19 Pandemic: Integrating the Health Belief Model (HBM) and Technology Continuous Theory (TCT). *Journal of Open Innovation: Technology, Market, and Complexity*, **7**, 132. <https://doi.org/10.3390/joitmc7020132>
- [22] Subaramaniam, K., Kolandaisamy, R., Jalil, A.B. and Kolandaisamy, I. (2020) The Impact of E-Wallets for Current Generation. *Journal of Advanced Research in Dynamical and Control Systems*, **12**, 751-759. <https://doi.org/10.5373/JARDCS/V12SP1/20201126>
- [23] Karim, M.W., Haque, A., Ulfy, M.A., Hossain, M.A. and Anis, M.Z. (2020) Factors Influencing the Use of E-Wallet as a Payment Method among Malaysian Young Adults. *Journal of International Business and Management*, **3**, 1-12.
- [24] Yesmin, S., Paul, T.A. and Uddin, M. (2019) bKash: Revolutionizing Mobile Financial Services in Bangladesh? In: Sikdar, A. and Pereira, V., Eds., *Business and Management Practices in South Asia*, Palgrave Macmillan, Singapore, 125-148. [https://doi.org/10.1007/978-981-13-1399-8\\_6](https://doi.org/10.1007/978-981-13-1399-8_6)
- [25] Ahmed, M.T., Imtiaz, M.T. and Kauser, A.A. (2020) A Comparative Study of Mobile Banking in Specific Parts of Bangladesh. *International Journal of Science and Business*, **4**, 129-139.
- [26] Rashid, M.H. (2020) Prospects of Digital Financial Services in Bangladesh in the Context of Fourth Industrial Revolution. *Asian Journal of Social Science*, **2**, 88-95. <https://doi.org/10.34104/ajssls.020.088095>
- [27] Mohd, S. and Pal, R. (2020) Moving from Cash to Cashless: A Study of Consumer Perception towards Digital Transactions. *PRAGATI: Journal of Indian Economy*, **7**, 1-13. <https://doi.org/10.17492/pragati.v7i1.195425>
- [28] Kumari, N. and Khanna, J. (2017) Cashless payment: A Behaviourial Change to Economic Growth. *Qualitative and Quantitative Research Review*, **2**, 84-90.

- [29] Singh, A., Srivastava, R. and Singh, Y.N. (2019) Prevention of Payment Card Frauds Using Biometrics. *International Journal of Recent Technology and Engineering (IJRTE)*, **8**, 516-525. <https://doi.org/10.35940/ijrte.C1106.1083S19>
- [30] Maddi, N.S. (2018) EMV Chip and PIN: A Feeble Upgrade.
- [31] Shareef, M.A., Baabdullah, A., Dutta, S., Kumar, V. and Dwivedi, Y.K. (2018) Consumer Adoption of Mobile Banking Services: An Empirical Examination of Factors According to Adoption Stages. *Journal of Retailing and Consumer Services*, **43**, 54-67. <https://doi.org/10.1016/j.jretconser.2018.03.003>
- [32] Malaquias, R.F. and Hwang, Y. (2019) Mobile Banking Use: A Comparative Study with Brazilian and US Participants. *International Journal of Information Management*, **44**, 132-140. <https://doi.org/10.1016/j.ijinfomgt.2018.10.004>
- [33] Hassan, H.E. and Wood, V.R. (2020) Does Country Culture Influence Consumers' Perceptions toward Mobile Banking? A Comparison between Egypt and the United States. *Telematics and Informatics*, **46**, Article ID: 101312. <https://doi.org/10.1016/j.tele.2019.101312>
- [34] Baabdullah, A.M., Alalwan, A.A., Rana, N.P., Kizgin, H. and Patil, P. (2019) Consumer Use of Mobile Banking (M-Banking) in Saudi Arabia: Towards an Integrated Model. *International Journal of Information Management*, **44**, 38-52. <https://doi.org/10.1016/j.ijinfomgt.2018.09.002>
- [35] Shankar, A. and Jebarajakirthy, C. (2019) The Influence of e-Banking Service Quality on Customer Loyalty: A Moderated Mediation Approach. *International Journal of Bank Marketing*, **37**, 1119-1142. <https://doi.org/10.1108/IJBM-03-2018-0063>
- [36] Anon (2022) Digital Currency vs Cryptocurrency—What's the Difference? <https://www.cnbctv18.com/cryptocurrency/digital-currency-vs-cryptocurrency--whats-the-difference-12611902.htm>
- [37] Anon (2022) What Is a Central Bank Digital Currency? Board of Governors of the Federal Reserve System. <https://www.federalreserve.gov/faqs/what-is-a-central-bank-digital-currency.htm>
- [38] Cisco (2008) Cyber Attack—What Are Common Cyberthreats? <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>
- [39] OWASP (2021) OWASP Top 10:2021. <https://owasp.org/Top10>
- [40] IBM (2021) What Is Cybersecurity? <https://www.ibm.com/topics/cybersecurity>
- [41] (2020) Twitter Hack: Staff Tricked by Phone Spear-Phishing Scam. BBC News. <https://www.bbc.com/news/technology-53607374>
- [42] (2021) Irish Health Cyber-Attack Could Have Been Even Worse, Report Says. BBC News. <https://www.bbc.com/news/technology-59612917>
- [43] Dong, S., Abbas, K. and Jain, R. (2019) A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. *IEEE Access*, **7**, 80813-80828. <https://doi.org/10.1109/ACCESS.2019.2922196>
- [44] Tidy, J. (2022) Ukraine Crisis: "Wiper" Discovered in Latest Cyber-Attacks. BBC News. <https://www.bbc.com/news/technology-60500618>
- [45] Wlazlo, P., Sahu, A., Mao, Z., Huang, H., Goulart, A., Davis, K. and Zonouz, S. (2021) Man-in-the-Middle Attacks and Defense in a Power System Cyber-Physical Testbed. *IET Cyber-Physical Systems: Theory & Applications*, **6**, 164-177. <https://doi.org/10.1049/cps2.12014>
- [46] (2016) Thousands of Popular Sites' at Risk of Drown Hack Attacks. BBC News. <https://www.bbc.com/news/technology-35706730>
- [47] IBM (n.d.) What Is a Cyber Attack? IBM. <https://www.ibm.com/topics/cyber-attack>

- [48] OWASP (2021) A03 Injection—OWASP Top 10:2021. [https://owasp.org/Top10/A03\\_2021-Injection](https://owasp.org/Top10/A03_2021-Injection)
- [49] (2015) Five Million Customers Affected by Vtech Database Hack. BBC News. <https://www.bbc.com/news/technology-34963686>
- [50] owasp.org (2021) A07 Identification and Authentication Failures—OWASP Top 10:2021. [https://owasp.org/Top10/A07\\_2021-Identification\\_and\\_Authentication\\_Failures](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures)
- [51] Kumar, V. and Sinha, D. (2021) A Robust Intelligent Zero-Day Cyber-Attack Detection Technique. *Complex & Intelligent Systems*, 7, 2211-2234. <https://doi.org/10.1007/s40747-021-00396-9>
- [52] Carnegie Endowment for International Peace (2016) Timeline of Cyber Incidents Involving Financial Institutions. <https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline>
- [53] Altwairqi, A.F., AlZain, M.A., Soh, B., Masud, M. and Al-Amri, J. (2019) Four Most Famous Cyber Attacks for Financial Gains. *The International Journal of Engineering and Advanced Technology*, 9, 2131-2139. <https://doi.org/10.35940/ijeat.B3601.129219>
- [54] Nasir, R., Afzal, M., Latif, R. and Iqbal, W. (2021) Behavioral Based Insider Threat Detection Using Deep Learning. *IEEE Access*, 9, 143266-143274. <https://doi.org/10.1109/ACCESS.2021.3118297>
- [55] Mohapatra, H., Rath, S., Panda, S. and Kumar, R. (2020) Handling of Man-in-the-Middle Attack in WSN through Intrusion Detection System. *International Journal of Emerging Trends in Engineering Research*, 8, 1503-1510. <https://doi.org/10.30534/ijeter/2020/05852020>
- [56] Zebari, R.R., Zeebaree, S.R., Sallow, A.B., Shukur, H.M., Ahmad, O.M. and Jacksi, K. (2020) Distributed Denial of Service Attack Mitigation Using High Availability Proxy and Network Load Balancing. 2020 *International Conference on Advanced Science and Engineering (ICOASE)*, Duhok, 23-24 December 2020, 174-179. <https://doi.org/10.1109/ICOASE51841.2020.9436545>
- [57] Kabalci, E. and Kabalci, Y. (2019) From Smart Grid to Internet of Energy. Academic Press, Cambridge. <https://doi.org/10.1016/B978-0-12-819710-3.00009-0>
- [58] Jain, S., Choudhari, P. and Srivastava, A. (2021) The Fundamentals of Internet of Things: Architectures, Enabling Technologies, and Applications. In: Balas, V.E. and Pal, S., Eds., *Healthcare Paradigms in the Internet of Things Ecosystem*, Academic Press, Cambridge, 1-20. <https://doi.org/10.1016/B978-0-12-819664-9.00001-6>
- [59] Camacho-Cogollo, J.E., Bonet, I. and Iadanza, E. (2020) RFID Technology in Health Care. In: *Clinical Engineering Handbook*, Academic Press, Cambridge, 33-41. <https://doi.org/10.1016/B978-0-12-813467-2.00004-3>
- [60] Singh, M.M., Adzman, K.A.A.K. and Hassan, R. (2018) Near Field Communication (NFC) Technology Security Vulnerabilities and Countermeasures. *International Journal of Engineering & Technology*, 7, 298-305.
- [61] Isravel, D.P., Arulkumar, D., Raimond, K. and Issac, B. (2020) A Novel Framework for Quality Care in Assisting Chronically Impaired Patients with Ubiquitous Computing and Ambient Intelligence Technologies. In: Peter, J.D. and Fernandes, S.L., Eds., *Systems Simulation and Modeling for Cloud Computing and Big Data Applications*, Academic Press, Cambridge, 61-79. <https://doi.org/10.1016/B978-0-12-819779-0.00004-6>
- [62] Rainer, R.K. and Prince, B. (2021) Introduction to Information Systems. John Wiley & Sons, Hoboken.

- [63] Masalha, F. and Hirzallah, N. (2014) A Students Attendance System Using QR Code. *International Journal of Advanced Computer Science and Applications*, **5**, 75-79. <https://doi.org/10.14569/IJACSA.2014.050310>
- [64] Din, M.M., Anwar, R.M. and Fazal, F.A. (2021), March. Asset Tagging for Library System—Does QR Relevant? *Journal of Physics: Conference Series*, **1860**, Article ID: 012017. <https://doi.org/10.1088/1742-6596/1860/1/012017>
- [65] Haber, M. (2021) Council Post: I Don't Scan QR Codes, and Neither Should You. *Forbes*. <https://www.forbes.com/sites/forbestechcouncil/2020/06/01/i-dont-scan-qr-codes-and-neither-should-you/?sh=11131f7251d1>
- [66] Chang, J.H. (2014) An Introduction to Using QR Codes in Scholarly Journals. *Science Education*, **1**, 113-117. <https://doi.org/10.6087/kcse.2014.1.113>
- [67] Narayanan, A.S. (2012) QR Codes and Security Solutions. *International Journal of Computer Science and Telecommunications*, **3**, 69-72.
- [68] (n.d.) QR Codes Are a Privacy Problem—But Not for the Reasons You've Heard. *Washington Post*. <https://www.washingtonpost.com/technology/2021/10/07/are-qr-codes-safe>
- [69] Ahuja, S. (2014) QR Codes and Security Concerns. *International Journal of Computer Science and Information Technologies*, **5**, 3878-3879.
- [70] Vauclair, M. (2011) Secure Element. In: van Tilborg, H.C.A. and Jajodia, S., Eds., *Encyclopedia of Cryptography and Security*, Springer, Boston, 46-59. [https://doi.org/10.1007/978-1-4419-5906-5\\_303](https://doi.org/10.1007/978-1-4419-5906-5_303)
- [71] Nosedá, M., Zimmerli, L., Schläpfer, T. and Rüst, A. (2021) Performance Analysis of Secure Elements for IoT. *IoT*, **3**, 1-28. <https://doi.org/10.3390/iot3010001>
- [72] Deshpande, V., George, L. and Badis, H. (2019) Pulsec: Secure Element Based Framework for Sensors Anomaly Detection in Industry 4.0. *IFAC-PapersOnLine*, **52**, 1204-1209. <https://doi.org/10.1016/j.ifacol.2019.11.362>
- [73] Türkmen, C. and Değerli, A. (2015) Transformation of Consumption Perceptions: A Survey on Innovative Trends in Banking. *Procedia—Social and Behavioral Sciences*, **195**, 376-382. <https://doi.org/10.1016/j.sbspro.2015.06.337>
- [74] Prakash, N. (2015) Host Card Emulation. *International Journal of Scientific and Research Publications*, **5**, 1-3.
- [75] Lepojevic, B., Pavlovic, B. and Radulovic, A. (2014) Implementing NFC Service Security—SE VS TEE VS HCE. *SYMORG Conference*, Zlatibor, 6-10 June 2014, 1-5.
- [76] Berlato, S. and Ceccato, M. (2020) A Large-Scale Study on the Adoption of Anti-Debugging and Anti-Tampering Protections in Android Apps. *Journal of Information Security and Applications*, **52**, Article ID: 102463. <https://doi.org/10.1016/j.jisa.2020.102463>
- [77] Appdome (2021) Mobile Banking App Security Requirements for 2022. <https://www.appdome.com/blog/mobile-banking-app-security-requirements>
- [78] Dong, S., Li, M., Diao, W., Liu, X., Liu, J., Li, Z., Xu, F., Chen, K., Wang, X. and Zhang, K. (2018) Understanding Android Obfuscation Techniques: A Large-Scale Investigation in the Wild. In: Beyah, R., Chang, B., Li, Y.J. and Zhu, S.C., Eds., *International Conference on Security and Privacy in Communication Systems*, Springer, Cham, 172-192. [https://doi.org/10.1007/978-3-030-01701-9\\_10](https://doi.org/10.1007/978-3-030-01701-9_10)
- [79] Park, M., You, G., Cho, S.J., Park, M. and Han, S. (2019) A Framework for Identifying Obfuscation Techniques applied to Android Apps Using Machine Learning. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Ap-*








- plications*, **10**, 22-30.
- [80] Cao, C., Tang, Y., Huang, D., Gan, W. and Zhang, C. (2021) IIBE: An Improved Identity-Based Encryption Algorithm for WSN Security. *Security and Communication Networks*, **2021**, Article ID: 8527068. <https://doi.org/10.1155/2021/8527068>
- [81] Ali, G., Ally Dida, M. and Elikana Sam, A. (2020) Two-Factor Authentication Scheme for Mobile Money: A Review of Threat Models and Countermeasures. *Future Internet*, **12**, 160. <https://doi.org/10.3390/fi12100160>
- [82] Kellner, A., Horlboge, M., Rieck, K. and Wressnegger, C. (2019) False Sense of Security: A Study on the Effectivity of Jailbreak Detection in Banking Apps. 2019 *IEEE European Symposium on Security and Privacy*, Stockholm, 17-19 June 2019, 1-14. <https://doi.org/10.1109/EuroSP.2019.00011>
- [83] Zhang, X.G., Yang, G.H. and Wasly, S. (2021) Man-in-the-Middle Attack against Cyber-Physical Systems under Random Access Protocol. *Information Sciences*, **576**, 708-724. <https://doi.org/10.1016/j.ins.2021.07.083>
- [84] Huang, J., Backes, M. and Bugiel, S. (2021) A11y and Privacy Don't Have to Be Mutually Exclusive: Constraining Accessibility Service Misuse on Android. 30<sup>th</sup> *USENIX Security Symposium (USENIX Security21)*, 11-13 August 2021, 3631-3648. <https://www.usenix.org/conferences/byname/108>
- [85] Lipovský, R., Štefanko, L. and Engineer, D. (2018) Android Ransomware: From Android Defender to Doublelocker. ESET Technology, 6-10.
- [86] Ichioka, S., Pouget, E., Mimura, T., Nakajima, J. and Yamauchi, T. (2020) Accessibility Service Utilization Rates in Android Applications Shared on Twitter. In: You, I., Ed., *International Conference on Information Security Applications*, Springer, Cham, 101-111. [https://doi.org/10.1007/978-3-030-65299-9\\_8](https://doi.org/10.1007/978-3-030-65299-9_8)
- [87] Leguesse, Y., Vella, M., Colombo, C. and Hernandez-Castro, J. (2020) Reducing the Forensic Footprint with Android Accessibility Attacks. In: Markantonakis, K. and Petrocchi, M., Eds., *International Workshop on Security and Trust Management*, Springer, Cham, 22-38. [https://doi.org/10.1007/978-3-030-59817-4\\_2](https://doi.org/10.1007/978-3-030-59817-4_2)
- [88] Possemato, A., Lanzi, A., Chung, S.P.H., Lee, W. and Fratantonio, Y. (2018) Clickshield: Are You Hiding Something? Towards Eradicating Clickjacking on Android. *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Toronto, 15-19 October 2018, 1120-1136. <https://doi.org/10.1145/3243734.3243785>
- [89] Ren, C., Liu, P. and Zhu, S. (2017) WindowGuard: Systematic Protection of GUI Security in Android. In NDSS. <https://doi.org/10.14722/ndss.2017.23529>
- [90] Salat, J., Setiawati, C.L. and Khalid, Z. (2021) Ku-Band Low Noise Block Converter (LNB) Sync Application Design Using Android Based Solid Dish. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)*, **4**, 1135-1150. <https://doi.org/10.33258/birci.v4i1.1725>
- [91] Appdome (n.d.) How to Prevent Malicious Misuse of Android Debug Bridge (ADB). <https://www.appdome.com/how-to/mobile-fraud-prevention/prevent-android-ios-fraud/block-adb>
- [92] Anon (2017) Download Magisk Manager Latest Version 24.2 for Android 2022. <https://magiskmanager.com>
- [93] Rao, V.V. and Chakravarthy, A.S.N. (2016) Analysis and Bypassing of Pattern Lock in Android Smartphone. 2016 *IEEE International Conference on Computational Intelligence and Computing Research (ICCIIC)*, Tamil Nadu, 15-17 December 2016, 1-3. <https://doi.org/10.1109/ICCIIC.2016.7919555>



- [94] Sun, S.T., Cuadros, A. and Beznosov, K. (2015) Android Rooting: Methods, Detection, and Evasion. *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, Denver, 12 October 2015, 3-14. <https://doi.org/10.1145/2808117.2808126>
- [95] Gunasekera, S. (2020) Rooting Your Android Device. In: Gunasekera, S., Ed., *Android Apps Security*, Apress, Berkeley, 73-223. [https://doi.org/10.1007/978-1-4842-1682-8\\_8](https://doi.org/10.1007/978-1-4842-1682-8_8)
- [96] FRIDA (n.d.) A World-Class Dynamic Instrumentation Framework. <https://frida.re>
- [97] D'Elia, D.C., Coppa, E., Palmaro, F. and Cavallaro, L. (2020) On the Dissection of Evasive Malware. *IEEE Transactions on Information Forensics and Security*, **15**, 2750-2765. <https://doi.org/10.1109/TIFS.2020.2976559>
- [98] Yin, X., Liu, S., Liu, L. and Xiao, D. (2018) Function Recognition in Stripped Binary of Embedded Devices. *IEEE Access*, **6**, 75682-75694. <https://doi.org/10.1109/ACCESS.2018.2883973>
- [99] Ravnås, O.A.V. (2019) Frida: Dynamic Instrumentation Toolkit for Developers, Reverse-Engineers, and Security Researchers.
- [100] Dresel, L., Protsenko, M. and Müller, T. (2016) Artist: The Android Runtime Instrumentation Toolkit. 2016 11th *International Conference on Availability, Reliability and Security (ARES)*, Salzburg, 31 August-2 September 2016, 107-116. <https://doi.org/10.1109/ARES.2016.80>
- [101] Druffel, A. and Heid, K. (2020) DaVinci: Android App Analysis beyond Frida via Dynamic System Call Instrumentation. In: Zhou, J.Y., et al., Eds., *International Conference on Applied Cryptography and Network Security*, Springer, Cham, 473-489. [https://doi.org/10.1007/978-3-030-61638-0\\_26](https://doi.org/10.1007/978-3-030-61638-0_26)
- [102] Albrecht, M.R., Blasco, J., Jensen, R.B. and Mareková, L. (2021) Mesh Messaging in Large-Scale Protests: Breaking Bridgefy. In: Paterson, K.G., Ed., *Cryptographers' Track at the RSA Conference*, Springer, Cham, 375-398. [https://doi.org/10.1007/978-3-030-75539-3\\_16](https://doi.org/10.1007/978-3-030-75539-3_16)
- [103] Zeb, S., Mahmood, A., Khowaja, S.A., Dev, K., Hassan, S.A., Qureshi, N.M.F., Gidlund, M. and Bellavista, P. (2022) Industry 5.0 Is Coming: A Survey on Intelligent NextG Wireless Networks as Technological Enablers.
- [104] Sarfraz, Z., Sarfraz, A., Iftikar, H.M. and Akhund, R. (2021) Is COVID-19 Pushing Us to the Fifth Industrial Revolution (Society 5.0)? *Pakistan Journal of Medical Sciences*, **37**, 591. <https://doi.org/10.12669/pjms.37.2.3387>
- [105] Chin, S.T.S. (2021) Influence of Emotional Intelligence on the Workforce for Industry 5.0. *Journal of Human Resources Management Research*, **2021**, Article ID: 882278.

## Annex

**Table A1.** [Full Form]. Cybersecurity affairs.

Cybersecurity	Interpretation	Instance
 <b>Phishing</b>	<ul style="list-style-type: none"> <li>• A state of social engineering</li> <li>• Spurious endeavor to acquire tactful information including login data, credit card info, and so on</li> <li>• Using email, messages as a medium</li> </ul>	<ul style="list-style-type: none"> <li>❖ An attack of spear-phishing against Twitter personnel accessing the account of some celebrity</li> </ul>
 <b>Malware</b>	<ul style="list-style-type: none"> <li>• One sort of malicious software</li> <li>• Allowing unauthorized entrance to the server, computer, network, etc.</li> <li>• malware comprising worms, adware, viruses, spyware, Trojan horses, ransomware, malicious bots, and so on</li> </ul>	<ul style="list-style-type: none"> <li>❖ A ransomware attack upon the health service of Ireland blocked the employees away from their associated computer systems</li> </ul>
 <b>DDoS attacks</b>	<ul style="list-style-type: none"> <li>• An attack aimed by zombies, bots</li> <li>• An endeavor to collapse a server, network, machine by encumbering it through traffic</li> <li>• through the medium of the simple network management protocol (SNMP)</li> </ul>	<ul style="list-style-type: none"> <li>❖ Distributed denial of service (DDoS) attacks emerged on numerous websites of banks and departments of the government of Ukraine</li> </ul>
 <b>Man In The Middle</b>	<ul style="list-style-type: none"> <li>• An attack of eavesdropping</li> <li>• It's seemed to be a usual interaction of information by eavesdropping or simulating devices</li> <li>• Injection of false data and commands are performed by the introducer</li> </ul>	<ul style="list-style-type: none"> <li>❖ The warning of the vulnerability of eavesdropping is reported for the numerous famous website</li> </ul>
 <b>Injection</b>	<ul style="list-style-type: none"> <li>• Injection of malevolent code inside the application for obtaining the data of the user</li> <li>• The concatenation of Hostile data is exploited</li> <li>• SQL, Object Relational Mapping, NoSQL, LDAP, OS command, Object Graph Navigation Library injection are usually familiar injections</li> </ul>	<ul style="list-style-type: none"> <li>❖ Through the SQL injection, around 5 million clients' databases of Vtech were hacked</li> </ul>
 <b>Authentication &amp; Identification</b>	<ul style="list-style-type: none"> <li>• Authentication—A technique of ensuring authorized entrance only into the elements of a system</li> <li>• Identification—A technique of identifying a system's user unambiguously</li> <li>• Controlling the authorization of logging, sessions of communication, handling of passwords, access of the system</li> <li>• Few examples of authentication can be Cipher Block Chaining Message Authentication Code, Hash-based Message Authentication Code</li> </ul>	<ul style="list-style-type: none"> <li>❖ After beginning the COVID-19 pandemic, a surprising expansion of cyber-attacks are executed on staff, and email scams of WHO. Then, WHO emigrated pretentious systems to the better-protected authentication system</li> </ul>
 <b>Zero-Day Attack</b>	<ul style="list-style-type: none"> <li>• Unknown susceptibility of any system which is concerned to manipulate with malevolent actions</li> <li>• Until architects determine the blunders, the exposures could be continued over days or a few months, even years</li> <li>• Without awareness of the security, the software version is released</li> </ul>	<ul style="list-style-type: none"> <li>❖ The zero-day attacks emerged on the File Transfer Appliance (FTA) of Accellion. The confidential data owned by the clients were embezzled through the attacker</li> </ul>

## Continued

**Cryptography**

- Conversion of Information or plaintext to ciphertext or assemble them invulnerable, protected against various cyber-attack
  - Two significant portions of algorithms for cryptography:
  - The encryption—the method of encoding information in such a manner from transmitters to recipients that none pretender can apprehend
  - The decryption—the contrary method of encryption, accomplished by secret key
  - Cryptographic breakdown emerges: lacking authenticated encryption of the data, absence of powerful and state-of-the-art algorithms as well as protocols, usages of FTP and SMTP for the conveyance of tactful data
- ❖ It's foreseen that quantum computer would damage the encryption of bitcoin

**Insider Threats**

- Vicious hazards inside the organization from present or past staffs, developers or members
  - It's a deliberate deception activity where private or monetarily beneficial information is the larceny
  - Conventional cyber security strategy (detection system, firewalls) are inadequate to detect insider threats
- ❖ In accordance with the “2020 Cost of Insider Threats study” of the Ponemon Institute, the mean yearly expenditure of interior violations of data was USD 11.45 millions where about 63% of these circumstances were imputed by dereliction