IDENTIFICATION AND PREVENTION OF IDENTITY THEFT

Al-Buxoriy Madinaxon
Biznes va turizmni rivojlantirish bo'limi menejeri, Toshkentdagi Singapur Menejmentni Rivojlantirish Instituti

https://doi.org/10.5281/zenodo.14736087

Innovations in advanced data transmission pathways, security protocols, physiological understanding, and software enhancements are always underway. Various processes and conceptual frameworks are required to protect information based on the methods of data transmission. As high-speed Internet access technologies evolve, essential business elements are transitioning to online platforms. Bank-client systems, corporate websites, e-commerce platforms, news outlets, entertainment services, trading platforms, blogs, and government portals are fundamental to the internet. Web applications are susceptible to attacks because of their accessibility, hence increasing the need for web application security solutions. Security necessitates data protection, since certain assets are tangible and possess monetary value, while others are intangible but nevertheless significant. Safeguarding tangible assets, such as the company's property register, user, customer, and employee information, as well as electronic currency, is vital. Nonetheless, intangible assets such as a company's image must be safeguarded. The protection of personal data is the foremost challenge and responsibility in information security globally and inside a business. Given that the majority of persons engage in online purchasing, e-commerce presents a unique challenge regarding the privacy of personal data on the internet. When executing these acts, meticulously assess the location from where the things are procured for legal conformity. Job search websites and portals providing customised services to the public may potentially jeopardise personal data. This program aims to determine the most effective methods for safeguarding Internet-exposed personal information. This article discusses personal data protection, breaches, and unauthorised third-party use resulting from their actions. Theft, distortion, manipulation, media deletion, and unauthorised access are examples. First, delineate the purpose of personal data prior to its protection. These measures limit businesses' unauthorised use and processing of personal data and mitigate the risk of breaches. This statute characterises personal data as any identifiable information pertaining to corporate clients and employees. Name, identification number, IP address, etc. This study examines general and sensitive personal data. Personal data such as employment, income, education, phone number, and identification number may identify an individual. The protection of personal data entails the establishment of local laws for managing personal data and the implementation of organisational and technical means to safeguard it. An automated solution cannot comprehensively delineate the personal data protection protocol inside an e-commerce firm, considering its specific context. Establishing personal data security protocols requires considerable time and effort. A competent institutional employee or third-party expert is required, resulting in additional expenses. Enhanced copying and dissemination technologies need the protection of personal data. Information technology has advanced to a point where the self-protection of information rights is no longer feasible in the face of privacy intrusions. Contemporary folks can no longer evade the extensive array of technological devices that collect and evaluate data on them. This research examines the selection of organisational and technical strategies for personal data processing. They inhibit illegal access,

deletion, modification, obstruction, and replication of personal data. The objective of these measures is to avert personal data breaches and related offences. This document examines the intricacies of information system software development and the safeguarding of personal data. This research aims to assess techniques for preventing Internet fraud. This work addresses contemporary cyberbullying prevention strategies, including antivirus software capable of identifying and categorising dubious messages as spam. The research investigates the economic challenges confronting people and businesses as a result of cybercrime. The primary emphasis will be a retrospective assessment of current situations. The paper analysed the criteria and measures required to safeguard the data of e-commerce web services. The website security system, a component of the web service, was examined independently. The most vulnerable and attractive targets for hackers, as well as areas of most concern, are under investigation. Instances of vulnerabilities, their consequences, attack pathways, and defensive strategies are presented (Laptiev et al., 2021). The primary types of assaults are analysed, with particular focus on resource-compromising attacks. A comprehensive analysis of the most pragmatic cybersecurity solutions and concepts for an integrated approach in software development is presented. This paper advocates for the use of technical and organisational protective measures. This document monitors software development and ongoing projects. Fabiano (2019) advocates for a source code security audit to scrutinise each line of code for vulnerabilities. A penetration test is sometimes referenced to identify flaws related to business logic, access differentiation, authentication, and session management. The auditor must circumvent all application security protocols to access sensitive data. The development dynamics of contemporary Internet projects, together with frequent modifications such as new functionalities, code revisions, and infrastructure enhancements, generate untested areas that may be susceptible to vulnerabilities. Consequently, the research advocates for yearly assessments and log surveillance of security incidents. Additionally, it incorporates Web Application Firewalls (WAFs) and vulnerability scanners as components of a comprehensive plan to defend against various attacks. Supplementary tools are evaluated. If security protections are testable and the actual IP address is disclosed, the tool is deemed untrustworthy (Deng, 2019). The initiative also gathers information on software testing service enhancements, dangerous configurations, open ports, and exposed vulnerabilities that might jeopardise user data. In conclusion, the study aims to identify the optimal personal data protection strategy for online trading processes. Project Significance: Despite the pandemic's disruption and unpredictability, individuals recognised that they were expected, and at times mandated, to provide personal information to combat COVID-19. Transitioning the majority of essential processes to the Internet in standard mode may take over a year. Extensive advancements that have transformed communication and engagement in the digital realm have created challenges in privacy protection for businesses aiming to adhere to legal standards and mitigate the crisis while safeguarding individual rights. Consumers and the public are increasingly apprehensive about the use of personal data. Data privacy is emerging as a significant issue for the majority of companies. In 2020, over fifty percent of data professionals from large and medium-sized multinational firms said their organisations needed to implement more data security measures (Clifford et al., 2018). The remote relocation of many employees and illicit activation may need additional safeguards. The pandemic has heightened the significance of privacy and the benefits of enhanced security for enterprises. Senior management and boards get data protection guidance. The company leader decides on privacy enhancements, making their participation essential. Senior management must

prioritise secrecy, since it is a fundamental principle of business. Numerous organisations use their data protection specialists to resolve these problems (Kodapanakkal et al., 2020). Consumers are increasingly apprehensive about data security in technologies used for remote purchases, communication with e-commerce platforms, and payment connections. The drastic workflow alterations and other repercussions of COVID-19 have compromised the integrity of IT infrastructure protection. Inefficient remote access to e-commerce platforms, VPN vulnerabilities, and insufficient personnel to address these issues jeopardise firm data. Consequently, the formulation of innovative personal data security protocols and the routine assessment of outdated technologies are essential. This study and effort in this domain are vital due to the emergence of advanced phishing tactics designed to obfuscate users and complicate the detection of attacks. The Emotet bot employs email interception as a very innovative mass phishing technique (Kuner et al., 2018). The bot utilises data from compromised e-sales services to dispatch fraudulent emails. This data is used in communication, making it persuasive and prompting victims to download malware files. Targeting high-level executives with whaling poses far greater risks. Cybercriminals may use personal information obtained or stolen online to dispatch persuasive fraudulent communications to company email accounts (Kodapanakkal et al., 2020). Simultaneously, hackers use trendy topics to entice victims into opening malicious emails. This may include COVID vaccination data, financial advisories, or political instability. The attitudes of leaders on personal and commercial data security are essential. Study Questions: The primary objective of the study is to address the enquiries, "What are the most common types of credit card fraud, and what are the most effective protective measures against it?" What are the approaches for risk reduction? Do the components of diamond fraud theory apply to internet fraud? » The effect of credit card fraud on companies will also be shown. The impact will be assessed using three methods. The financial losses, the most apparent consequence of fraud on a corporation, will be measured. Secondly, it will be shown how fraud diminishes a company's standing among investors and partners. The paper will also examine "How does credit card fraud distort data?" The inquiry will concentrate on the security of online purchases. Comprehending the mechanisms of credit card theft is essential for combating it. The study will address the question, "What are the causes of contemporary card fraud, the mechanisms involved, and the vulnerabilities in the protection systems that facilitate it?" The two most common forms of card account theft will be explored. The first method excludes cardholders when card data is extracted en masse from banks, online retailers, and online service providers. Typically, organised criminals or cybercriminals are involved. Funds are disbursed when card information is sold on online criminal platforms. The cardholder-assisted fraud methodology will be examined next. Individual fraudsters sometimes use sophisticated social engineering techniques to manipulate human behaviour. They perpetrate theft with techniques that exploit human weak spots. This analysis will explore the mechanisms of prevalent plastic card thefts and the most effective prevention strategies. The analysis will include skimming, shimming, re-debiting from the card, data interception, and data theft facilitated by Trojans and viruses. The subsequent study subject is "What are the solutions for the organisation of intellectual property, particularly software?" Their organisation will focus on the impact of protecting software on cyberattacks and card forgeries that result in payment theft. The evolution and enhancement of fraud techniques will be explored. Historically, skimmers were only located on ATMs, or little cameras were positioned nearby to capture the PIN digits of plastic bank cards. Currently, keyboard pads are the most prevalent, with an integrated keyboard and a top panel that resembles it while allowing for PIN

code entry. The paper must address the future of prominent cyber fraud trends and their impact on the global economy and industry. Conceptual Framework: Any data related, either directly or indirectly, to a legal entity is classified as personal data. Customer data includes identification number, exact address, mobile phone number, and email address, as stated by Yartey et al. (2021). The processing of information systems generates new risks that must be mitigated or eradicated. Threats to information are internal or external factors affecting an automated processing system that might jeopardise data subjects. Morse et al. provide a contextual enumeration of scenarios in which information systems are vulnerable (2020). It transpires when the company's software is antiquated, defective, and susceptible. The likelihood of threats increases if certain system functions, particularly defensive measures, are ineffective or if information operation and storage are challenging. The implementation of specific protective strategies in this research is contingent upon various security levels, as noted by Hou et al. (2019). The criteria delineate protective levels for each category of danger: maximum, high, medium, and low. The characteristics of Wagner affect its selection (Wagner, 2018). The quantity of subjects whose data is processed, together with the classification and value of the processed data, is prioritised. Sun et al. additionally include types of processing and the significance of threats (Sun et al., 2018). Evaluating these attributes facilitates the development of a system capable of addressing data security threats at all anticipated levels. Besides technology, the protective system integrates many methods. Regulatory mandates require businesses to safeguard personal data. Technical and organisational measures are implemented. This paper will delineate cyber fraud as the leakage, loss, distortion, and destruction of customer personal data (Whitty, 2019). Adherence to personal data protection standards necessitates the development, implementation, and maintenance of advanced software systems that execute the following functions (Ivanov et al., 2018): This obstructs both external and internal attackers from gaining access to data. Firewalls, access control systems, encryption, and blocking are used for this purpose. The company autonomously determines all necessary methods to safeguard personal data from breaches, necessitating simply their competencies and certifications, rather than specific software names or types. Pérez-González et al. (2019) assert that the development of a data security system should be executed incrementally. Every project management method implements new tasks incrementally. These include development, testing, implementation, analysis, and modification to rectify deficiencies. The head of the organisation should supervise this array of duties. In this case, a personal data security system will function without modifications. Globalisation, the swift advancement of financial markets and the instruments traded therein, along with the intricacy of economic entities and their business operations, foster conditions conducive to the biased representation of public information, including corporate financial statements. The combination of these factors and the ethical transformation of the modern "homo economicus" engenders novel corporate deceit. They progressively do not align with Cressy's differential association theory, or FTT (Zadereyko et al., 2019). The three-factor FTT model was subsequently augmented to include "abilities." A superior model, The Diamond Fraud Theory (FDT), emerged almost fifty years later. The fraudster needs the capability to more effectively navigate FTT situations. It is necessary to justify and conceal unethical actions concerning the falsification of the company's public information. Project Limitations: The effort is constrained by its incapacity to collect credible cyber fraud statistics, since it can only rely on data breaches reported by regulators. Merely 10–12% of cybercrimes are documented (Ali et al., 2018). Individuals and organisations that have experienced online extortion

are apprehensive about seeking professional help due to the risks associated with disclosing compromised information. Perpetrators continually devise novel methods to illicitly acquire sensitive data, which cannot be overlooked. More than 20 types of software exist that incapacitate networked devices (Harvey, 2018). Hackers continually enhance their techniques and have long used artificial intelligence, complicating threat detection systems. Fraudsters also devise novel techniques for extracting payment information. Client profiles of online shops include identification, address, telephone number, and banking card details. Trends in data security often evolve and cannot be fully comprehended. Artificial intelligence represents a new frontier in the prevention of cyber fraud. AI-driven solutions will gain prominence as businesses transition from data centres to cloud environments. Online retailers may use enhanced security configurations due to ongoing advancements in surveillance and safeguarding. The Data Leak Prevention system is used to detect and avert the unauthorised dissemination of purchasers' private information via both internal and external channels in real time. Users' end devices may also be managed using it. This study is also constrained by the inability to foresee all security failures and internal vulnerabilities. This study only impacts significant trading organisations equipped with comprehensive risk monitoring systems and a wide array of threats. Limited research has gathered and assessed external impact threats for small and medium-sized e-commerce firms. Human error, a significant contributor to data breaches, is another limitation. Employee neglect and noncompliance with essential security protocols may undermine even the most reliable information security measures. Most intentional actions are driven by financial incentives. In large businesses, certain employees may engage in misconduct if they see an opportunity. Regrettably, individuals in the material-valued department are at risk. Both business data (including customer bases, supplier bases, and marketing tactics) and consumer personal data are significant. Certain employees see corporate data as personal, which contributes to its release; departing individuals often believe they may maintain access to it. The diamond fraud theory posits that Internet fraudsters may be driven by data rather than financial gain. An SSL certificate on the website is perhaps the most effective method to protect credit card information. The SSL certificate safeguards client data in online shops, including names, addresses, phone numbers, and bank card information (Wang et al., 2020). Consequently, hackers are unable to access this information and use it to misappropriate funds from a client's card. Furthermore, each edition of the program is presumably more reliable. Developers revise software with each iteration, rectifying vulnerabilities exploited by hackers. Non-updatable plugins, extensions, and applications expose e-commerce sites on independent platforms to hacker vulnerabilities. Regularly updating website and server software with the latest minor security versions may be the most effective and straightforward method to avert an attack. Consequently, obtaining the latest browser update and updating the computer's operating system should prevent data breaches associated with device malfunctions. Mitigating hacking risks involves the constant monitoring of service security warnings and the implementation of security patches. The optimal technique for securing data transmission is expected to align the site with global e-commerce standards. Consistent security scans, reliable backups, and reputable hosting will suffice. Any business that accepts credit or debit cards, whether online or offline, is required to adhere to the guidelines set by the PCI Security Guidelines Council (Wilson et al., 2018). These standards protect corporate financial information. Violations of regulations increase the danger of customer data breaches. Selecting the appropriate hosting provider may protect an e-commerce company. Dedicated servers, due to their enhanced security, are likely to perform optimally. Virtual

services and hosting are the least effective because of their standardised plans, which lack customisation for individual shops. Hosting providers must conduct frequent backups, maintain comprehensive records, and oversee network activities. The warning system for account irregularities and site infections is essential. Technical help should notify of the infringement and provide instructions along with a link to the knowledge base for resolution. The use of plugins and firewall software may also influence the situation. Firewalls also obstruct internet threats such as cross-site scripting and SQL injection (Latchoumi et al., 2020). Implementing two-factor authentication upon login will enhance security. All individuals are required to provide supplementary information that is exclusively known to them. This effectively protects the online store's website against credit card data leaks.DefinitionsAccess control systems organise and limit data access using software and hardware (Hirsch, 2018).Taylor (2020) defines antivirus software as a program that prevents, detects, and eliminates computer infections.According to Becerril (2018), specialised software may stop the transfer of secret information and monitor employee work to identify security vulnerabilities and avoid breaches.During a certain expiry date, a card user has the legal right to use a plastic card for financial transactions (Zadereyko et al., 2019).Maintaining confidentiality is crucial to avoid unauthorised access by other parties (Wang et al., 2019).Fraudulent credit card usage may lead to illicit withdrawal of cash and misuse of personal data (Bertrand et al., 2020).According to Mariani et al. (2021), cryptographic protection involves data change via encryption and/or extension creation.The card may include bank account information such as the owner's name, number, expiry date, and security code (Laptiev et al., 2021).The Diamond fraud hypothesis outlines four factors that fraudsters need to commit theft: opportunity, motive, ability, and justification. 2019 (Zadereyko et al.).Fabiano (2019) defines e-commerce as the distribution, advertising, marketing, and selling of products or services online.An external invader is someone outside the information system during threat implementation (Deng, 2019).A firewall is a computer software that protects against viruses and hacker assaults (Clifford et al., 2018).Internet fraud known as fishing involves obtaining user identity data (Kodapanakkal et al., 2020).Kuner et al. (2018) define identity theft as the fraudulent exploitation of personal data to steal money or get advantages.Yartey et al. (2021) define information security vulnerabilities as deficiencies in an asset or control and management system that attackers may exploit.Information storage involves storing source data to provide timely data supply upon user request (Morse et al., 2020).An insider is an invader in the information system during a threat implementation (Hou et al., 2019).Information leakage over a technical channel refers to the uncontrolled transfer of protected information from a carrier to a technological interceptor (Wagner, 2018).Sun et al. (2018) define level of protection as the effect of technological and organisational measures on information safety and security.According to Whitty (2019), personal data refers to any information that may identify an individual.According to Ivanov et al. (2018), re-debiting involves withdrawing money from a bank card twice for the same transaction.Shimming is an advanced kind of skimming that involves reading a bank customer's card information at an ATM using a thin device (Pérez-González et al., 2019).Skimming is a sort of bank card fraud that involves skimming information from the magnetic stripe using a tech device or skimmer (Ali et al., 2018).According to Wang et al. (2020), a Trojan is a harmful software used by attackers to steal information, damage computers, disrupt performance, or misuse resources.Wilson et al. (2018) define unauthorised access/actions as violating established rights and norms for accessing or using information.A virus is a tiny software that infects executable files, file allocation blocks, or the boot sector of media and

documents prepared with office programs (Latchoumi et al., 2020).SummaryThe Internet symbolises globalisation, which was explained in the first chapter. The globalisation of Internet users is increasing the popularity of online shops. As a communication hub, it orchestrates network commerce elements. The advantages of the Internet extend beyond international trade. Globalisation has resulted in data breaches, which are elucidated. It is transpiring at an unparalleled velocity, and e-commerce experts may encounter it at any moment. Recent statistics indicate many data breaches that undermine brand confidence. The project's objective is to delineate stages of cyber fraud prevention, prevalent causes, and the effectiveness of preventative remedies. The research must include a method for attributing data related to different types of credit card theft. The project's contribution to the popularisation of online shopping during the COVID-19 pandemic and retail mall closures is also acknowledged. In response to the increasing prevalence of online consumers, new fraudulent schemes have surfaced, necessitating enhanced security protocols. This study will examine these issues. Initially, it is essential to identify the most prevalent types of credit card theft, evaluate the efficacy of various protective measures, and explore strategies to mitigate risk. The theories and terminology pertinent to this study align with the research questions. This section of the first chapter comprises robust arguments and credible comments from scientists. These theoretical sources illuminate credit card data security. Subsequently, the project's limitations are addressed, primarily owing to the rapid escalation of cybercrime and emerging fraud tactics. Owing to ongoing breakthroughs in protective measures, there are an excessive number to address in a single volume. Assumptions include those related to the greatest and least effective protective techniques. The list of effective measures is extensive and encompasses several technology methods. Ineffective methods are sometimes associated with a too broad and non-tailored protection strategy. The first chapter concludes with a list of definitions. The semantic domains include "Types of credit card fraud," "Methods of personal data protection," "Confidentiality," and "Electronic commerce." Ultimately, a conclusion encapsulates the first chapter and preceding content. Procedures and Method Introduction The empirical aspect of the research entails using authors' expertise to identify deficiencies, weaknesses, and threats to information and software system security and protective measures. The expertise derived from certification and state examinations, case studies, and security audits of over 500 information security tools, products, portals, and systems in the secure execution by prominent international and American developers (Eslamkhah et al., 2019) underscores the necessity and hyper-complexity of assessing IT product information security compliance amidst the significant escalation in the complexity and dynamism of IT products. Software system security persists as an unresolved issue despite the commendable efforts of esteemed engineers (Baldassarre et al., 2020). Critical vulnerabilities persist, making code analysis a challenging task that must be addressed continuously throughout the software system's life cycle. Information security systems are mostly governed via tool certification. Professionals at testing laboratories and certifying bodies must coordinate and deliberate to implement practical solutions. This study aims to utilise appropriate procedures, measurements, and methodological approaches, which may prove highly valuable. The significant societal interest in this topic in America over recent years necessitates consideration of technical development, encompassing various social phenomena. In light of the inevitability of personal data regulation, all legal entities in the country have modified their strategies for safeguarding private information and its implications (Walters et al., 2018). Manufacturers of security products must adhere to certification rules in the American computer

security industry owing to competitive certification practices. This paper delineates conformity assessment via the use of international standards in the practical section. It encompasses the assessment of information security compliance. The certification of information security tools and their associated legal and regulatory framework are delineated below. Practical work entails using mathematical models and procedures to substantiate test results and facilitate task planning (Mamonova et al., 2020). It also provides formalised testing and information protection protocols in accordance with both traditional and contemporary regulatory standards. The practical component of this article will evaluate security protection compliance to ascertain if the requirements for products, processes, and systems are met. Kurpayanidi (2019) characterises conformity assessment as the processes of testing, control, certification, and accreditation. This chapter will use several conformity assessment methodologies. Conformity assessment operations in information security include certification of information systems, testing, and control in accordance with established standards. Software, information systems, and information security management systems may undergo audits to evaluate information security. The most effective conformity assessment techniques for technological means and protection systems include testing, certification, auditing, and risk analysis, along with the certification of information security tools. Testing is an evaluative procedure for conformity evaluation. Experiments are used to ascertain the quantitative or qualitative characteristics of the test object throughout its operation, modelling, or effects. Certification authenticates the data processing capabilities of informatisation facilities. Certification exams, which meticulously evaluate the safeguarded information, constitute its fundamental essence. This transpires in real operational contexts to ascertain that the enacted procedures and protective strategies comply with information security requirements. Certification assessments confirm that the informatisation object satisfies program efficacy criteria. It first safeguards data against unwanted access, including computer viruses. Specialised devices incorporated into information technology products inhibit leakage and exposure (Kamalieva et al., 2020). Software testing identifies issues and deficiencies in the implementation of software properties. Contemporary software development incorporates testing inside the software quality management system across the whole life cycle. International standards define testing as a technical procedure that assesses one or more attributes of a product, process, or service using an authorised method. In the practical segment, the synthesis of the specified approaches for demonstrating the effectiveness of information security instruments will be used. Project Design for Research: Initially, choose the most critical testing areas from the comprehensive list to implement the project. The methodology for assessing software security vulnerabilities must be established. Consequently, it will be possible to discern a vulnerable blind spot for further data expropriation. The enforcement of access control regulations must be verified. It intercepts both explicit and implicit requests, precisely distinguishing between permitted and unauthorised requests based on specific and mandatory criteria. Note that vulnerability testing differs from manual testing. Vulnerability testing detects flaws, whereas manual testing rectifies them. Manual penetration testing (pentests) safely infiltrates the online store's infrastructure to assess its security (Ghanem et al., 2019). This may occur via operating system, service, or application vulnerabilities, improper configurations, or negligent user conduct. The organisation is under assault to see whether hackers can infiltrate them. The test results indicate the extent of potential infiltration by an attacker and the volume of data they may extract or exploit. A series of measures is required to monitor and identify system and software vulnerabilities in the event of illicit third-party

interference, unauthorised access, and data replication. This is an examination of data privacy. Consequently, many complimentary verification techniques should be used (Panchekha et al., 2019). Security testing will concentrate on mitigating risks to the integrity of systems, software, and personal data. Security measures include assessing the resilience of applications and programs against viruses, spyware, hacking attempts, and malware. Select the most effective tool for managing payment banking systems in e-commerce platforms. Evaluate the safety of private data using the designated tools. A subsequent requirement is a compilation of programs that restrict third-party user access to certain information. They must also validate data integrity, including application, software, and segment self-recovery after unforeseen failures. The nature of the applications under evaluation dictates the requisite security level; hence, criteria must be defined. White, grey, and black box methodologies may be used to enhance software security (Park, 2019). White box testing presupposes that the user is familiar with the system's functionalities and idiosyncrasies. Grey boxes exhibit limited awareness, but black boxes do not possess any awareness. Each method has distinct results and effectiveness. Criteria must be set to determine the most suitable solution for a certain circumstance. Code static analysis, vulnerability and bug searches, and product certification readiness evaluations must be conducted consistently. Sampling procedures are established, and the optimal Internet data protection solutions from four categories are selected. This includes antivirus software, firewalls, network intrusion prevention and alert systems, and vulnerability assessment tools. Classic, proactive, and integrated antivirus software is available. Traditional antivirus systems use signatures to detect recognised pathogens. Proactive virus prevention systems defend the system against infection; integrated programs use both methods. This analysis examines linked programs, since they constitute the bulk of the market. Corporate programs may deploy updates for several users from an internal server, in contrast to personal programs. Consequently, in the selection of antivirus software, real-time virus and Internet threat prevention using cloud technologies, as well as a module for Internet payment security, were taken into account. The use of antivirus packages was influenced by the availability of platforms (Windows, Android, Mac OS) (Shah et al., 2021). The malware and adware detection speed of the site and major apps was evaluated. The sample was assembled using several criteria, since firewalls prevent computer threats, in contrast to antiviruses. The simplicity of setup and the presence of a training mode are the key prerequisites for a firewall. Applications must promptly terminate network attacks, oversee traffic from installed applications, detect viruses and malware, and obstruct advertisements during payment transactions. The specified firewalls were required to protect the store's webpages from attacks, viruses, and malicious code while addressing various vulnerabilities that could jeopardise client security (Kaplan et al., 2019). The designated utility must also oversee the incoming and outgoing traffic of other applications. The Internet connection will be immediately blocked if the process seems dubious. Programs should have many major modules or components to tailor protection according to use. These firewalls offered adaptable network traffic regulation, rule formulation, and password-secured configurations. Subsequently, a prototype of Data Loss Prevention (DLP) systems (software or hardware-software integrations) was developed to prevent unauthorised disclosure of confidential information outside the corporate network. The sample focused on the effectiveness of business and external data flow analysis. The response rate was evaluated based on whether a pre-established regulation or policy governed the transfer of sensitive information. The system obstructed transfers or notified security personnel at a certain moment. The control subsystem architecture dictates the kind of DLP system: network,

agency, or hybrid (Guzairov et al., 2018). Network solutions use centralised data traffic monitoring by transmitting mirrored copies to specialist servers for analysis in accordance with security protocols. Analysing just network traffic complicates the comprehension of user management of private information. Analysts indicate that encrypted data constituted over 60% of worldwide web traffic in 2019, with the increasing use of messengers, cloud services, and other specialist information exchange apps complicating leak protection in the absence of workplace oversight (Dmitriev, 2020). Consequently, only hybrid software complexes were selected. The most recently developed sample includes vulnerability scanners. The global vulnerability scanner business is expanding. These tools currently serve as project-orientated vulnerability management solutions. Ultimately, vulnerability monitoring initiatives include several departments. We used contemporary scanners integrated with risk management, patch management, incident management platforms, and secure development protocols for our inquiry. Data Sources: Without a comprehensive analysis of all components of the specified instruments' activities, the protection of e-commerce processes cannot be validated. Extensive quantities of hand-obtained primary data may be erroneous. Erroneous data used for decision-making may jeopardise the protective mechanism. The volume of primary data also influences the comprehensiveness and precision of the protection strategy. Automated data collection and processing techniques are used due to their speed, accuracy, and reduced labour requirements. Numerous tools serve as preset information sources for these automated processes. Initially, these sensors monitor the program's response time to system anomalies. These devices assess system issues. The majority of data was obtained during static testing. Malware scanning on demand is implemented. A static test was conducted on several malware files to get pertinent information. The tests used samples from the preceding six months and assessed hard disc on-demand results. Products were examined across many domains for certification, including the identification of all viruses on the list that might jeopardise customers' financial information (Noeiaghdam, 2019). The program must detect and eliminate viruses from the system. Statistical observation was used to document facts and their indicators characterising the efficacy of Internet security measures against bank data breaches, following a singularly planned program. In the first observation, a monitoring program was established, including a catalogue of data-gathering sites along with relevant indications and indicators. The performance criteria from the Sampling Procedure section were integrated. The form also included viral detection status, heuristic analysis, false positive rates, and treatment for current infections. The ratio of harmful objects to analysed files established the detection threshold. Heuristic analysis facilitated the identification of signatures and the detection of updated viruses even when the signature does not completely align with the characteristics of an unknown program, provided that there are broader indicators of a virus present in the suspicious program (Sing et al., 2021). This method may elevate false positives; hence, newer applications use it judiciously. The ratio of false positives was evaluated for collections including several non-malicious files. The quantity of false positives and their proportion relative to the overall file count were then calculated. A blank monitoring program was used to enter primary data and technical specifications of the studies. Instructions detailing the tests and the parameters under investigation at this step were crucial for completing the form. Consequently, a statistical aggregate was compiled as a set of indicators for information data security technologies, sharing a similar qualitative foundation (program objective) while possessing unique characteristics. Consequently, homogeneous, dynamic, independent data units were acquired. Reaction rate data was gathered from minute samples, in

contrast to static testing. In a specific kind of response rate testing, larger, however still small, test sets were used to illustrate the general indicators of each antivirus provider. Furthermore, specific malware discoveries were not disclosed. In a separate assessment, each sample was evaluated individually. Dynamic testing sought to replicate the genuine user environment for the evaluated security system using all available methodologies. The properties of the new security tool, which are inapplicable in a typical testing environment, make its need more apparent. The closest test to real-world conditions indicated that the malware detection efficacy of some solutions was inferior to their detection rates while analysing infected files on demand. The dynamic testing findings were validated for dependability and completeness as primary statistical data. Electronic commerce information security practitioners were interviewed for the practical aspect of the study. During the interview, they examined their preferred security protocols for specific businesses and their strategies to prevent bank data breaches. The interview questions addressed information risk analysis techniques and the challenges associated with the installation, configuration, and maintenance of technical information security measures. Every online trading company employs IT personnel. They perform various positions based on a company's operations, specialism, and responsibilities. The respondents included computer security experts from many fields. Security engineers provide comprehensive security throughout the organisation. They provide security training and recommendations for internal employee groups, assess security solutions, assist in personnel selection, and conduct information security management. A cybersecurity specialist verifies the efficacy of the company's software security measures. A seasoned cloud security engineer safeguards databases inside digital cloud infrastructures. Information security auditors specialise in assessing susceptible systems. The optimal structure for banking information security and data processing was investigated with operational security personnel. Network and Internet security specialists addressed enquiries on safeguarding all business computers from viruses and malware. Application security professionals were sought after for their expertise in mobile app resilience. An interview with recovery specialists, who assist post-attack, was essential. They preferred rapid data security techniques to mitigate espionage, prevent data breaches, and eliminate viruses. The extensive interview segment was designed for all electronic commerce information security specialists to identify their preferred hacking tools. Defining the workplace's direction and specifics was also necessary. The frequency of use of certified and licensed programs was subsequently revealed. Motivations and factors were evaluated while choosing a client data protection solution. The interview included leading questions on browser client deficiencies and web application vulnerabilities. The third segment of the discussion with e-commerce information security experts addressed the mitigation of real-world threats. The first component addressed undesirable content: information-accessing products and instruments. These technologies include malware and perilous connections. Enquiries ensued about combating hackers, intercepting communications, and preventing data theft. A fraudster's hacking and a victim's inadvertent provision of access may both result in unauthorised entry. The most significant aspect was the experience with fraud, particularly with the use of technology to embezzle funds. This segment included the acquisition of personal data, usernames, passwords, and credit card information, as well as the use of surveys and questionnaires. Currently, online retailers are integral to commercial enterprises. Iavich et al. indicate that hundreds of attacks transpire daily on small corporate websites, with over 40% of hacking incidents occurring in this context (2019). In light of rapid expansion and a competitive landscape, several organisations prioritise security. Following

interviews with information security professionals, surveys were conducted with corporate executives to gather data. This survey determined the least effective security measures, which should be excluded from the final evaluation (Torten et al., 2018). The management was interrogated over the adequacy of the online store's security protocols. Online store proprietors were also enquired about their readiness for the escalating instruments of assailants and their apprehensions about potential future assaults. Their experiences in gathering confidential information, especially personal data, and infiltrating their company's information systems were scrutinised. Research was conducted on hacker attacks targeting business web and mobile applications. The adverse impacts of security vulnerabilities on e-commerce sector executives were assessed. The website was deemed unreachable after the installation of a malicious script by attackers that altered the page content. A foreign text is shown instead of the product catalogue. The survey revealed that customers abandoned purchases and shifted to competitors while the team rehabilitated the site after a hacking incident. Upon the infiltration of security information into the network, it disseminates rapidly; hence, the exodus of the audience was also analysed. Regaining brand trust is challenging after a certain duration (Wilis et al., 2020). Online consumers will only make purchases if they have confidence in the enterprise. Upon the reporting of security concerns, some users transfer to competitors. The poll assessed the level of confidence the target audience has in the respondents' stores. Additionally, the survey results identified the requisite pricing and quality for information security managers. To elucidate this figure, it was determined who is responsible for information security inside the business (Norbekov, 2020). A dedicated, full-time structural unit inside an information security organisation was proposed as the preliminary option. The second answer came from an individual or many personnel external to the information security section. Managers of electronic stores with security provided by a third-party information protection service were required to choose the third option. The poll excluded managers from firms that do not safeguard data. Subsequently, managers selected the professional qualifications of their information security personnel from the provided list. Proposals were made for the automation of security information analysis, computer system and network security, and the protection of automated system information. Identifying, averting, and eradicating cyberattacks, together with the technological safeguarding of information, technologies, and labour organisation, were viable alternatives, as were economic, geopolitical, and social transformations. If respondents replied affirmatively, they were prompted to forecast new information security positions inside the business. Subsequently, management needed to choose if they would replace equipment in the next year. A list of potential positions was included to streamline the task, including analysts in extensive data security, intricate cyberattack detection, and system security. Experts in information security specialising in data analysis for fraud detection, artificial intelligence, distributed ledger technology security, and computer incident response were also viable responses. The research enquired of managers on their desired protective measures, emphasising the significance of robust indicators. Document analysis data was examined by Liu et al. via penetration testing and an information security assessment (Liu et al., 2021). He demonstrated that shortcomings in web application protection remain a significant information security concern. Attackers often use web application vulnerabilities to steal information and infiltrate commercial information systems. Nirmal's data indicate that XSS attacks, SQL injections, anomalous circumstances, CSRF forgeries, and malware infections pose the greatest threats to web application security (Nirmal et al., 2021). The subsequent literature source demonstrates that web application protection must

account for specific factors intrinsically linked to its functionality (Kim et al., 2021). Consequently, users, customers, and partners must have round-the-clock access to the online store's website and web applications, including payment functionalities. Abideen et al. (2019) assert that firewalls and SSL do not safeguard online applications against attacks. The site must remain accessible from external networks. Manual discovery and remediation of vulnerabilities in applications, websites, or online portals often proves ineffective, as noted by Li et al. (2020). Developers may identify and fix several vulnerabilities, while an attacker needs just a single weakness to prevail. The document analysis indicates that primary security for the online store's website must be included throughout the design and payment application development phases. Timely updates during operation are essential. Bavel et al. provide a web application security strategy based on an online store model, examining its functionality, vulnerabilities, and principal threats (Bavel et al., 2019). Every online shop is a web application linked to an e-commerce system; thus, the secure online store model must protect against fraud and unauthorised access to customers' financial information. This necessitates fraud prevention, payment data security, and online vulnerability safeguards. The subsequent research included two tests (Zeng et al., 2020). The first experiment investigated the impact of an assailant introducing malicious JavaScript code using a CSS attack to get the online store administrator's cookie. The second experiment of this article included modelling user registration and payment data to evaluate the efficacy of the payment data protection module. Each experiment started with the protection modules disabled, followed by a repetition with them enabled. The second experiment simulated online store user registration and payment data input into the database to evaluate the efficacy of the payment data protection module. When the payment data security module was disabled, the payment information of online shop customers was stored in the database unencrypted. Consequently, if an assailant acquires unauthorised access to the database, they will be able to seize the payment information of the online store's clientele. With the payment data protection module activated, the payment information of the online store's clients is kept in the database in an encrypted format. Consequently, if an assailant has unauthorised access to the online store's database (for instance, by exploiting server weaknesses), they will possess consumers' payment information in encrypted format. They will be unable to utilise them for their own objectives without employing cryptanalysis tools.

Focus Groups. The focus groups comprised five of the most prominent security applications within each category emphasised in the Sampling Procedure chapter.

Antivirus Software. The antivirus software market is currently vast, yet certain programs have solidified their presence in the market. Avast antivirus has consistently ranked among the top free malware protection software for numerous years (Nurhayati, 2019). It offers robust security, including an integrated VPN and gaming mode, can generate boot copies, and evaluates the risk of Wi-Fi networks. Antivirus Plus is among the most renowned antivirus solutions globally, created by the Romanian firm Bitdefender (Shedid et al., 2019). The arsenal includes a comprehensive array of capabilities to thwart any viral assaults. A specialised software core concurrently reduces CPU load, so averting performance decline during operation. Dr.Web CureIt operates swiftly and effectively, capable of detecting infections that standard antivirus programs would overlook (Uchenna et al., 2018). The tool will swiftly examine any disc, partition, or directory, enabling the user to selectively choose items for inspection. Kaspersky Lab frequently achieves top results in antivirus evaluations. This research analyses Kaspersky Security Cloud, which the business claims

represents a novel advancement in security, integrating two decades of accomplishments from Kaspersky Studio (Tchernykha et al., 2018). Given the proliferation of diverse malware in recent years compared to other threat categories, MalwareBytes is one of the most effective tools for combating it (Pisula, 2019). It enables the simultaneous scanning of the system for different viruses and their removal without disrupting site operations. Firewalls: According to the study by Movahedi et al., Windows is the most susceptible operating system, therefore justifying the need for built-in security (Movahedi et al., 2019). Alongside its renowned antivirus, Avast also offers a firewall, which is part of the premium suite of Avast Premium Security applications (McIntosh et al., 2019). It includes an antivirus, an anti-spam module, a wireless network protection module, and other capabilities. PeerBlock differs somewhat from the other firewall applications mentioned in the document. Rather than obstructing applications, PeerBlock restricts a compilation of IP addresses associated with certain categories (Abdi et al., 2020). For instance, it may download and obstruct a compilation of IP addresses identified as business suppliers, advertisers, spyware, etc. pfSense is a premier network firewall with commercial-grade features. It is an open-source security solution based on FreeBSD (Wada et al., 2021). Sophos is an emerging leader in the cybersecurity sector, and their software is an excellent choice for safeguarding enterprises. The XG Firewall Business Edition security technology is far more sophisticated than conventional firewall software (Stoynov et al., 2021). ZoneAlarm is a reputable firewall with a user-friendly interface (Muzammil et al., 2019). The user-friendly interface conceals numerous functions, including the selection of protection levels tailored to meet diverse business requirements. Tools for Preventing Network Attacks In the realm of intrusion prevention solutions, the product from Positive Technologies is featured (Arefin et al., 2020). The application executes all operations in real time without impacting the business's network activities. The next-generation firewall is an advancement above conventional firewalls, with the capability to oversee the state of connections. The primary producer of NGFW solutions used in this study is UserGate (Anlei et al., 2020). The document further introduces a proxy server equipped with information security capabilities, sometimes referred to as a web filter. Smart-Soft is engineered and refined to adhere to the company's online security protocols and regulate user access to websites (Mimura et al., 2018). To mitigate attacks aimed at vulnerabilities without established protection, there exists a category of network security solutions. Consequently, Cisco's primary responsibility is to examine the file sent across the network device for malicious code (Alfarsi et al., 2019). The InfoWatch data leak prevention system is the last in this focus group. It is intended to identify and avert possible breaches of data confidentiality and personal information, such as credit card numbers (Shabalin et al., 2020). Vulnerability scanning tools are essential instruments within information security departments, as new vulnerabilities emerge daily, creating potential risks for the organisation. The OpenVAS Vulnerability Scanner is a sophisticated tool for vulnerability analysis, enabling the scanning of servers and network devices (Dissanayaka et al., 2020). This scanner identifies an IP address and examines open services by probing open ports, misconfigurations, and vulnerabilities in existing entities. F-Secure Radar is a product of F-Secure, a firm engaged in the antiviral sector (Karantzas et al., 2021). Radar is a cloud-based solution that functions as both a vulnerability scanner and a platform for vulnerability and asset management. Astra is a comprehensive cloud-based VAPT tool specifically designed for e-commerce (Sodhi, 2020). It includes a suite of programs, malware, and network assessments to evaluate the security of a web application for processing payment orders. W3Scan is a complimentary console vulnerability scanner including over 1200 integrated plugins

(Muliński, 2020). They can identify fingerprints of web pages, assess port configurations, analyse website architecture, detect numerous prevalent vulnerabilities, and check for SQL Injection. Sn1per is a robust framework for automated target security assessment (Li et al., 2021). This project will include extensions such as Findsploit (for rapid identification of exploits related to vulnerabilities) and PrivEsc (for the detection of local issues). Observations: The test was executed on a specifically configured platform using VMware Workstation. A pristine virtual computer with the Microsoft Windows XP SP2 operating system was replicated for each antivirus product (Singh et al., 2018). All activities indicated by the antivirus product, including system reboot and updates, were executed during installation. The antivirus settings were unchanged and stayed at their default configuration. A distinct clean virtual computer was designated for each antivirus product. The compilation stored on an external hard drive was examined. The scanning of a directory containing virus samples designed to exfiltrate banking information was initiated on request in each evaluated antivirus program. The five chosen antivirus programs exhibited the following malware detection rates: Avast: 95.52%; Plus: 78.27%; Dr.Web CureIt: 89.46%; Kaspersky Security Cloud: 96.49%; MalwareBytes: 56.02%. Subsequently, a firewall assessment was performed, wherein a security testing application was initiated to evaluate the efficacy of the firewall software. The firewall test included the examination of a series of rules, namely the evaluation of manual rules inside a firewall. During testing, the software attempted to exploit ports using certain network protocols to access financial data. Upon completion of the software, a report was produced detailing the susceptible ports and protocols inside the network. The Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Money Transfer Protocol (MTP) were evaluated (Akanji et al., 2012). This procedure was created to thoroughly examine all open ports on the network, perhaps numbering in the thousands. The quantity of used ports inspected by each firewall was recorded as follows: Avast: 863; PeerBlock: 874; pfSense: 812; XG Firewall Business: 844; ZoneAlarm: 930. The last phase included evaluating solutions to mitigate network threats. During the examination, controlled penetrations were conducted to ascertain the thoroughness and accuracy of the intrusion report. The detectors gathered event data and used several metrics to ascertain that the analysed activity diverged from the usual. Ten controlled assaults were executed using five distinct methodologies used in attacks on remote banking payment systems. Each tool recorded the quantity of unauthorised login attempts. The frequency with which the tools successfully disrupted access to mobile banking was estimated out of 10 attempts. The following findings were recorded: Positive Technologies: 9; UserGate: 7; Smart-Soft: 7; Cisco: 9; InfoWatch: 8. In the concluding phase of the observation stage, a testing method was conducted to evaluate the performance of vulnerability scanners for e-commerce sites. The previously generated test material for functional verification of all technical requirements contains many vulnerabilities. The whole class of comparable vulnerabilities identified on the test site was regarded as a single vulnerability. Scanners with the specified configurations were deployed on the evaluated site, and a series of functional tests was conducted. Subsequently, the web objects identified by the scanner (distinct links, vulnerabilities, attack paths, etc.) were quantified and categorised. Observations yielded the following data on discovered vulnerabilities: OpenVAS Vulnerability Scanner: 75, 20%; F-Secure Radar: 79, 27%; Astra: 94, 24%; W9scan: 88, 46%; Sn1per: 90, 14%. Data analysis indicates that all chosen tools demonstrated a commendable degree of protection. Kaspersky Security Cloud and ZoneAlarm occupy the top place in the ranking, with scores of 96.49% and 930, respectively. The second place in the ranking is held by both Avast products, which have shown exceptional

performance. MalwareBytes antivirus software and OpenVAS Vulnerability Scanner ranked last and had the lowest efficacy, with results failing to surpass 80%. Consequently, four levels of control were delineated, and the programs and instruments pertinent to the investigation were allocated accordingly. Three primary layers of protection may be identified, focusing on software and hardware. The first-level technologies effectively identify and eliminate recognised viruses. Second-level programs effectively identify and eliminate unknown viruses, while the third level of protection includes a built-in function for blocking virus manifestations. The scanning method is most effective for detecting and eradicating known viruses. It involves identifying computer viruses using their distinctive segments of program code (signature, program strain). F-Secure Radar, Astra, W9scan, and Sn1per have effectively developed a scanning database including code fragments of recognised computer viruses. They conducted virus detection by comparing the data in the computer's memory with the established codes of the scanning database. Astra and Sn1per excelled at detecting and deciphering the coding of the new malware. They included the most quantity of viral signatures into the scanning database. The distinctive feature of F-Secure Radar was its capability to accurately repair and disinfect compromised segments of the electronic payment system. It is important to note that W9scan does not keep the signatures themselves; rather, it retains checksums or signature extensions. The deficiencies of the primary tools, particularly scanners, were ascribed to their capability to identify viruses that have already infiltrated computer systems, which have been analysed and for which a signature has been established. To ensure successful functioning, the scanning database must be regularly replenished. The detection and eradication of undiscovered viruses are essential to safeguard against those overlooked by the first tier of antivirus protection. The most efficient approach is system integrity monitoring (change detection), which is used by the majority of the tools examined in this research. Both antivirus software and firewalls effectively assessed and contrasted the present characteristics of the computer system with the reference parameters indicative of its uninfected condition. 80% of the examined tools effectively safeguarded the information resource against unauthorised alteration and destruction due to different forms of illicit interference, as well as system and environmental failures. Consequently, all tools for preventing network assaults (Positive Technologies, UserGate, Smart-Soft, Cisco, and InfoWatch) performed their functions at a comparable level, warranting their classification as second-tier solutions. Moreover, all antivirus programs and brandmasters uniformly succeeded in addressing the aforementioned second-level tasks. The highest tier of protection, which entails obstructing virus manifestations and safeguarding against harmful actions and replication of computer viruses that have surpassed the initial two levels of defence, can be ascribed to over fifty percent of the analysed antivirus solutions and firewalls. The techniques used by Avast, Dr.Web CureIt, and Kaspersky Security Cloud antiviruses, together with Avast, PeerBlock, XG Firewall Business, and ZoneAlarm firewalls, rely on the interception of virus-specific functionalities. Dr.Web CureIt and XG Firewall Business operate on the basis of program filtering, making them somewhat less effective than other products that function as hardware controls. In the context of worldwide public networks, particularly regarding consumer payments, third-level security systems conducted antivirus monitoring of all transmitted traffic. It may be executed via many methods: by deploying an antivirus proxy server or by including an antivirus module with a firewall. The drawbacks of these controllers include the absence of an autoconfiguration mechanism. Consequently, there exists a potential for conflicts with other system programs, including additional safety protection measures. Summary: The

chapter on methods and methodology started with an introduction delineating the research's stated aim. The context of the intricate procedures is established during which the functionality of technologies designed to safeguard the confidentiality of personal data for both the client and the seller will be evaluated and assessed. Subsequent to the introduction, the design of the research study was provided. This section provides a description of the research methodologies and algorithms used to address the objectives outlined in the study. Furthermore, it encompasses a delineation of the organisation and content of the study, including research procedures and criteria for assessing the study's outcomes. Subsequently, it provides a description of the sampling procedures essential for evaluating the quality of research subjects and ascertaining their characteristics through reliability metrics. The chosen samples will comprehensively represent the analysed composition indicators for the current timeframe. Furthermore, the principal criteria for sampling used in the composition of the work are discussed. Following the exposition of the sampling technique, the sources of data collection are delineated. This study employs a statistical technique, and the recommended procedure of direct observation is presented. The measuring and counting procedures used for the registration of the researched units are elucidated. This section includes details of a recorded observation that included gathering information via a literature study, followed by a description of a structured interview using open-ended questions performed with security experts in the e-commerce domain. The obligatory interview strategy, including the order of questions and their phrasing in an open format, was delineated. The response choices and the criteria for categorising the interviews into groups were standardised. Alongside interviews, a survey of e-commerce company executives was used as a tool for gathering primary information. It allowed for a written appeal to a designated group of individuals (respondents) using information security features in their application or on their website. The methodology for statistical processing and interpretation of the collected replies was established. The subsequent section of the third chapter included the compilation of theoretical material on data protection phenomena and processes using documentary sources. Data from the documents was retrieved and documented, thereafter used to investigate the research topic. The analysis of the documents examined characteristics and properties of security content in electronic commerce, serving as primary criteria for evaluating the protection level of bank data. The study includes four focus groups, with the first being antivirus software. The five most prevalent antivirus software solutions for securing IT infrastructure in the corporate e-commerce industry are delineated. Subsequently, a focus group of five firewalls is identified during the interview as the most effective tools for traffic regulation. This article delineates the primary functions performed by the firewalls discussed. The strategies and benefits of each of the five software applications are delineated. The significance of using tools to avert network assaults in business environments has been recognised for an extended period, so five analogous programs are included in the third focus group. The article identifies the manufacturers deemed most successful by the interview participants. The interview participants affirmed that data leaking occurred more often than monetary theft. This illustrates that the diamond fraud theory alters the motivational factors for offline fraudsters. It includes minor information on how a specific application addresses bypass technique and offers a concise overview of attack protection mechanisms. The identification of possible threats is a crucial phase in guaranteeing information security. Consequently, based on the feedback from the questioned IT professionals, a focus group including five prospective vulnerability scanners was assembled. A concise synopsis of each network scanner has been compiled, detailing the specific duties they are

designed to address. Additional insights about the evaluation of the chosen programs were provided. The procedure for evaluating each focus group is outlined, and the resulting indications are presented. This section provides the statistical data obtained from the analysis of the four categories of protection. The concluding section of the third chapter presents an analysis of the data acquired during the observation of the testing. Although some chosen applications demonstrated a high, third degree of data security protection, none proved to be entirely successful. Consequently, it may be inferred that the most dependable approach is to integrate many bank data security solutions simultaneously.

REFERENCES

1. Abdi, A., & Singh, G. (2020). Opportunities and challenges of the implementation of peer-to-peer blockchain technology in higher educational institutions. International Journal of Engineering Research & Technology, 9(5), 348-358. doi: 10.5860/crl.81.1.43
2. Abideen, M. Z., Saleem, S., & Ejaz, M. (2019). Advanced data security and its applications in multimedia for secure communication. Security and Communication Network, 9(15), 312-316. doi: 10.1155/2019/7924690
3. Akanji, O. S., Abisoye, O. A., & Iliyasu, M. A. (2021). Mitigating slow hypertext transfer protocol distributed denial of service attacks in software defined networks. Journal of Information and Communication Technology, 20(3), 277-304. doi: 10.32890/jict2021.20.3.1
4. Alfarsi, G., Tawafak, R. M., Alsidiri, A., Jabbar, J., Malik, S. I., & Alsinani, M. (2019). Using Cisco Packet Tracer to simulate a smart home. International Journal of Engineering Research & Technology, 8(12), 670-674. doi: 10.1007/s10586-017-1298-1
5. Ali, N. I., Samsuri, S., Seman, M. A., Brohi, I. A., & Shah, A. (2018). Cybercrime: An Emerging Challenge for Internet Users—An Overview. Sindh University Research Journal: Science Series, 50(3D), 55-58. doi: 10.1016/j.procs.2015.08.443
6. Anlei, W., Zhaoshun, W., & Shuwang, L. (2020). A fast, single pattern matching algorithm of next-generation firewall. International Journal of New Developments in Engineering and Society, 4(1), 33-40. doi: 10.25236/IJNDES.040106
7. Arefin, T., Uddin, R., Evan, N. A., & Alam, R. (2020). Enterprise network: Security enhancement and policy management using next-generation firewall (NGFW). Computer Networks and ISDN systems, 25(5), 280-310. doi: 10.29145/sir/22/020204
8. Baldassarre, M. T., Barletta, V. S., Caivano, D., & Scalera, M. (2020). Integrating security and privacy in software development. Software Quality Journal, 28(14), 987-1018. doi: 10.1007/s11219-020-09501-6
9. Bavel, R. V., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behaviour. International Journal of Human-Computer Studies, 123(6), 29-39. doi: 10.1016/j.ijhcs.2018.11.003
10. Becerril, A. (2018). The value of our personal data in the Big Data and the Internet of All Things Era. Advances in Distributed Computing and Artificial Intelligence Journal Regular Issue, 7(2), 71-80. doi: 10.14201/ADCAIJ2018727180
11. Bertrand, Y., Boudaoud, K., & Riveill, R. (2020). What do you think about your company's leaks? A survey on end-users perceptions toward data leakage mechanisms. Frontiers in Big Data, 8(5), 1-13. doi: 10.3389/fdata.2020.568257
12. Clifford, D., & Ausloos, J. (2018). Data protection and the role of fairness. Yearbook of European Law, 37(6), 130-187. doi: 10.1093/yel/yey004

13. Deng, M. I. (2019). Regulation and protection of personal data in the context of big data. Journal of Beijing University of Posts and Telecom, 21(1), 19-25. doi: 1019722/jcnki1008772920180176
14. Dissanayaka, A. M., Mengel, S., Gittner, L., & Khan, H. (2020). Security assurance of MongoDB in singularity LXCs: An elastic and convenient testbed using Linux containers to explore vulnerabilities. Cluster Computing, 23(2), 1955-1971. doi: 10.1007/s10586-017-1511-2
15. Dmitriev, D. D. (2020). Software and hardware complex for the development and research of methods for broadband access to multimedia resources and the Internet. Journal of Physics: Conference Series, 5(15), 1-7. doi: 10.1088/1742-6596/1515/3/032041
16. Eslamkhah, M., & Seno, S. A. (2019). Identifying and ranking knowledge management tools and techniques affecting organisational information security improvement. Knowledge Management Research & Practice, 26(3), 1-30. doi: 10.1080/14778238.2019.1599495
17. Fabiano, N. (2019). Ethics and the Protection of Personal Data. Systemics, cybernetics, and informatics, 17(2), 58-64. doi: 10.1145/3309772.3309787
18. Ghanem, M. C., & Chen, T. M. (2019). Reinforcement learning for efficient network penetration testing. Information, 11(6), 1-23. doi: 10.3390/info11010006
19. Guzairov, M., Gvozdev, V., Davlieva, A., & Teslenko, V. (2018). Analysis of properties of hardware-software systems in efficiency index under uncertainty component structures. Advances in Intelligent Systems Research, 6(4), 19-25. doi: 10.2991/iwci-18.2018.13
20. Harvey, L. A. (2018). REDCap: Web-based software for all types of data storage and collection. Spinal Cord, 56(625), 1282-1288. doi: 10.1038/s41393-018-0169-9
21. Hirsch, P.B. (2018). The goose that laid the golden eggs: personal data and the Internet of Things. Journal of Business Strategy, 40(1), 48-52. doi: 10.1108/JBS-10-2018-0176
22. Hou, H., Yua, J., & Hao, R. (2019). Cloud storage auditing with deduplication supporting different security levels according to data popularity. Journal of Network and Computer Applications, 134(4), 26-39. doi: 10.1016/j.jnca.2019.02.015
23. Iavich, M., Gnatyuk, S., Iashvili, G., & Fesenko, A. (2019). Cybersecurity European standards in business. Scientific and Practical Cyber Security Journal, 3(2), 36-39. doi: 10.1007/s11042-016-3495-y
24. Ivanov, V., Reznik, A., & Succi, G. (2018). Comparing the reliability of software systems: A case study on mobile operating systems. Information Sciences, 423(4), 398-411. doi: 10.1016/j.ins.2017.08.079
25. Kamalieva, L. A., Kazakova, I. A., Nikonovich, S. L., Goncharov, V. V., & Livson, M. (2020). Improving information security: Criminal-legal means of counteracting digital data leakage. Laplage em Revista, 6(1), 222-229. doi: 10.24115/S2446-622020206
26. Kaplan, D. E., & Rajendran, S. (2019). Firewalls in general relativity. Physical Review, 99(4), 1-8. doi: 10.1103/PhysRevD.99.044033
27. Karantzas, G., & Patsakis, C. (2021). An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(6), 387-421. doi: 10.3390/jcp1030021
28. Kim, Y., Wang, Q., & Roh, T. (2021). Do information and service quality affect perceived privacy protection, satisfaction, and loyalty? Evidence from a Chinese O2O-based mobile shopping application. Telematics and Informatics, 56(39), 568-575. doi: 10.1016/j.tele.2020.101483

29. Kodapanakkal, R. I., Brandt, M. J., Kogler, C., & Beest, I. V. (2020). Self-interest and data protection drive the adoption and moral acceptability of big data technologies: A conjoint analysis approach. Computers in Human Behaviour, 108(2), 10-16. doi: 10.1016/j.chb.2020.106303
30. Kuner, C., Cate, F. H., Lynskey, O., Millard, C., Loideain, N. N., & Svantesson, D. J. (2018). Expanding the artificial intelligence-data protection debate. International Data Privacy Law, 8(4), 289-292. doi: 10.1093/idpl/ipy024
31. Kurpayanidi, K. I. (2019). Theoretical basis of management of innovative activity of industrial corporations. International Scientific Journal of Theoretical & Applied Science, 69(1), 7-14. doi: 10.15863/TAS
32. Laptiev, O., Savchenko, V., Kotenko, A., Akhramovych, V., & Samosyuk, V. (2021). Method of determining trust and protection of personal data in social networks. International Journal of Communication Networks and Information Security, 13(1), 15-21. doi: 10.54039/ijcnis.v13i2.5034
33. Latchoumi, T. P., Reddy, M. S., & Balamurugan, K. (2020). Applied machine learning predictive analytics to SQL injection attack detection and prevention. European Journal of Molecular & Clinical Medicine, 7(2), 3543–3553. doi: 10.23919/INM.2017.7987433
34. Li, X., Wang, L., Xin, Y., Yang, Y., & Chen, Y. (2020). Automated vulnerability detection in source code using minimum intermediate representation learning. Applied Sciences, 10(16), 1-16. doi: 10.3390/app10051692
35. Li, Y., Cheng, J., Huang, J., Chen, Z., & Niu, W. (2021). NEDetector: Automatically extracting cybersecurity neologisms from hacker forums. Journal of Information Security and Applications, 169(58), 80-90. doi: 10.1016/j.jisa.2021.102784
36. Liu, S., Reviriego, P., Montuschi, P., & Lombardi, F. (2021). Less-is-Better Protection (LBP) for memory errors in kNN classifiers. Future Generation Computer Systems, 117(22), 401-411. doi: 10.1016/j.future.2020.12.015
37. Mamonova, G., & Maidaniuk, N. (2020). Mathematical tools for the Internet of Things analysis. Cybernetics and Systems Analysis, 56(15), 621-627. doi: 10.1007/s10559-020-00279-w
38. Mariania, M. M., Styven, M. E., & Teulon, F. (2021). Explaining the intention to use digital personal data stores: An empirical study. Technological Forecasting and Social Change, 166(2), 12-16. doi: 10.1016/j.techfore.2021.120657
39. McIntosh, T., Jang-Jaccard, J., Watters, P., & Susnjak, T. (2019). Masquerade attacks against security software exclusion lists. Australian Journal of Intelligent Information Processing Systems, 16(4), 1-8. doi: 10.1007/978-3-030-66218-9
40. Mimura, M., & Tanaka, H. (2018). Leaving all proxy server logs to paragraph vector. Journal of Information Processing, 26(38), 804-812. doi: 10.4018/978-1-4666-5888-2
41. Morse, W. C., Cox, C., & Anderson, C. J. (2020). Using public participation geographic information systems (PPGIS) to identify valued landscapes vulnerable to sea level rise. Sustainability, 12(6), 1-34. doi: 10.3390/su121767
42. Movahedi, Y., Cukier, M., Andongabo, A., & Gashi, I. (2019). Cluster-based vulnerability assessment of operating systems and web browsers. Computing, 101(4), 139-160. doi: 10.1007/s00607-018-0663-0
43. Muliński, T. (2020). ICT security in tax administration – Rapid7 Nexpose vulnerability analysis. Studia Informatica: Systems and Information Technology, 2(24), 37-51. doi: 10.34739/si.2020.24.03

44. Muzammil, A. C., & Nandan, R. (2019). Comparative analysis of packet filtering firewalls. International Journal of Scientific Research in Computer Science Applications and Management Studies, 8(5), 1-4. doi: 10.5334/dsj-2018-032
45. Nirmal, K., Janet, B., & Kumar, R. (2021). Analysing and eliminating phishing threats in IoT, networks, and other web applications using iterative intersection. Peer-to-Peer Networking and Applications, 14(4), 2327-2329. doi: 10.1007/s12083-020-00944-z
46. Noeiaghdam, S. (2019). A novel technique to solve the modified epidemiological model of computer viruses. SeMA Journal, 76(8), 97-108. doi: 10.1007/s40324-018-0163-3
47. Norbekov, J. (2020). Ensuring information security as an ideological problem. Mental Enlightenment Scientific-Methodological Journal, 1(39), 56-65. doi: 10.1002/ett.3815
48. Nurhayati, A. (2019). Mapping perception of consumer antivirus software with the multidimensional scaling method. Journal on Computer Science and Information Technologies, 4(3), 91-95. doi: 10.11591/APTIKOM.J.CSIT.13
49. Panchekha, P., Ernst, M. D., Tatlock, Z., & Kamil, S. (2019). Modular verification of web page layout. PROC Acm. Programming Language, 3(151), 1-26. doi: 10.1145/3360577
50. Park, S. (2019). Software requirement specification based on a grey box for embedded systems: A case study of a mobile phone camera sensor controller. Computers, 8(20), 1-11. doi: 10.3390/computers801002
51. Pisula, A. (2019). Enigma Software Group USA. Federal Communications Law Journal, 72(2), 272-275. doi: 10.1109/VTCSpring.2015.7146058
52. Pérez-González, C. J., Colebrook, M., Roda-García, J. L., & Rosa-Remedios, B. (2019). Developing a data analytics platform to support decision-making in emergency and security management. Expert Systems with Applications, 120(7), 167-184. doi: 10.1016/j.eswa.2018.11.023
53. Shabalin, A. M., & Kaliberda, E. A. (2020). Building a virtual model for corporate information protection using the InfoWatch traffic monitor system. Proceedings in Cybernetics, 67(1), 35-42. doi: 10.34822/1999-7604-2020-1-35-42
54. Shah, H., & Comissiong, D. M. (2021). Computer virus model with stealth viruses and antivirus renewal in a network with fast infectors. SN Computer Science, 407(3), 34-39. doi: 10.1007/s42979-021-00780-9
55. Shedid, M., Abdelmonem, M., Boraik, A., Elmetwalli, A., & Hassan, D. (2019). Safety parameters throughout the first month of direct-acting antivirus. American Journal of Technologies, 152(1), 16-19. doi: 10.1016/j.jss.2020.110609
56. Sing, P., & Kottath, R. (2021). An ensemble approach to meta-heuristic algorithms: Comparative analysis and its applications. Computers & Industrial Engineering, 162(48), 1-13. doi: 10.1016/j.cie.2021.107739
57. Singh, H., & Kumar, A. (2018). A review on Windows updates, security patches, and issues. International Journal of Emerging Technologies and Innovative Research, 5(10), 701-712. doi: 10.5120/ijca2015907209
58. Sodhi, H. S. (2020). An investigation for prioritising industry 4.0 tools using the analytic hierarchy process. International Journal of Advance Science and Technology, 29(10S), 5619-5629. doi: 10.1016/j.jisa.2021.102752
59. Stoynov, S., & Nikolov, B. (2021). Approach to SHIP'S IT and OT systems cybersecurity improvement. Pedagogika-Pedagogy, 93(7s), 185-196. doi: 10.53656/ped21-7s.16appr
60. Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., & Wang, G. (2018). Data processing and text mining technologies on electronic medical records: A review. Journal of Healthcare Engineering, 14(3), 1-9. doi: 10.1155/2018/4302425

61. Taylor, R. D. (2020). "Data localisation": The internet in the balance. Telecommunications Policy, 44(8), 132-135. doi: 10.1016/j.telpol.2020.102003
62. Tchernykha, A., Babenko, M., Chervyakov, N., Miranda-López, V., Kuchukov, V., Cortés-Mendoza, J., & Deryabin, M. (2018). AC-RRNS: Anti-collusion secured data sharing scheme for cloud storage. International Journal of Approximate Reasoning, 45(4), 1-16. doi: 10.1108/ILDS-07-2016-0026
63. Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behaviour. Computers & Security, 79(4), 68-79. doi: 10.1016/j.cose.2018.08.007
64. Uchenna, C. C., Roslee, M. B., & Nmenme, P. U. (2018). Android antivirus system for malware mutation in networking. Engineering International, 6(2), 63-78. doi: 10.1007/978-3-319-39510-4_25
65. Wada, I., Dawakinkudu, A. M., & Saka, K. A. (2021). Usability and challenges of pfSense deployed for management of library networks, servers, and users in State University of Science and Technology, Wudil. Jewel Journal of Librarianship, 16(3), 71-90. doi: 10.1016/j.acalib.2019.01.001
66. Wagner, J. (2018). The transfer of personal data to third countries under the GDPR: When does a recipient country provide an adequate level of protection? International Data Privacy Law, 8(4), 318-337. doi: 10.1093/idpl/ipy008
67. Walters, R., Zeller, B., & Trakman, L. (2018). Personal data law and competition law: Where is it heading? UNSW Law Research Journal, 18(73), 1-20. doi: 10.2139/ssrn.3275832
68. Wang, X., Continella, A., Yang, Y., He, Y., & Zhu, S. (2019). Leakdoctor: Toward automatically diagnosing privacy leaks in mobile applications. Proceedings of the ACM on Interactive Mobile Wearable and Wearable Ubiquitous Technologies, 3(28), 1-25. doi: 10.1145/3314415
69. Wang, Y., Xu, G., Liu, X., Mao, W., Si, C., Pedrycz, W., & Wang, W. (2020). Identifying vulnerabilities of SSL/TLS certificate verification in Android apps with static and dynamic analysis. Journal of Systems and Software, 167(4), 16-19. doi: 10.1016/j.jss.2020.110609
70. Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. Journal of Financial Crime, 26(1), 277-292. doi: 10.1108/JFC-10-2017-0095
71. Wilis, R. A., & Nurwulandari, A. (2020). The effect of e-service quality, e-trust, price, and brand image on e-satisfaction and its impact on the e-loyalty of Traveloka's customers. Jurnal Ilmiah Manajemen, Ekonomi, dan Akuntansi, 4(3), 1061-1099. doi: 10.1016/j.apmrv.2015.03.005
72. Wilson, D., Roman, E., & Beierly, I. (2018). PCI DSS and card brands: Standards, compliance, and enforcement. Cyber Security: A Peer-Reviewed Journal, 2(1), 73-82. doi: 10.1145/3314415
73. Yartey, D., Omojola, O., Amodu, L., Ndubueze, N., Adeyeye, B., & Adesina, E. (2021). Personal data collection and usage for mobile marketing: Customer awareness and perception. WSEAS Transactions on Business and Economics, 18(5), 42-50. doi: 10.37394/23207.2021.18.5
74. Zadereyko, O. V., Trofymenko, O. G., & Loginova, N. I. (2019). Algorithm of user's personal data protection against data leaks in Windows 10 OS. Informatics, Control, Measurement in Economy and Environmental Protection, 1(5), 41-44. doi: 10.5604/01.3001.0013.0905
75. Zeng, W., Bashir, R., Wood, T., Siewe, F., Janicke, H., & Wagner, I. (2020). How location-aware access control affects user privacy and security in cloud computing systems. EAI Endorsed Transactions on Cloud Systems, 6(18), 1-11. doi: 10.4108/eai.13-7