Lecture Notes in

Introduction to Data & Information Security

Assoc.Prof. Shimaa Ouf

Information Systems Department
Faculty of Commerce and Business Administration

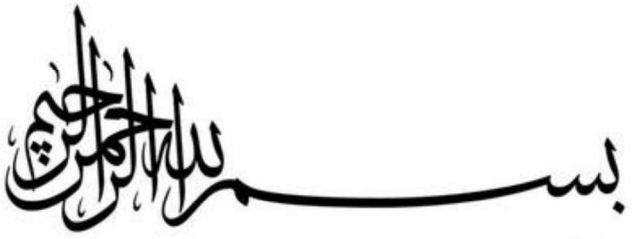
Helwan University

Dr. Soha Ahmed Ali

Information Systems Department
Faculty of Commerce and Business Administration

Helwan University

الناشر: جهاز نشر وتوزيع الكتاب الجامعي
2023



الناشر: جهاز النشر وتوزيع الكتاب الجامعي

السنة الميلادية (2023 – الفصل الدراسي الأول)

Important Note

The following lecture notes are gathered from different open sources, scientific papers, and publications, also gathered from trusted websites.

Preface

Organizations rely heavily on the use of information technology (IT) products and services to run their day-to-day activities. Ensuring the security of these products and services is of the utmost importance for the success of the organization. As well as, keeping data and communications secure is one of the most important topics in development today. This lecture note is designed specifically for undergraduate Business Information Systems (BIS) students. It comprises the information that will be presented in the lectures as well as selected subjects that are linked to the introduction to Data Security studies. It was compiled from and created utilizing a variety of sources that were edited, summarized, and explained using well-known scientific processes. Its sole objective is to assist students in understanding what will be described in lectures as well as in locating these discussed subjects in one material and presenting them in an easy and appropriate manner.

Table of Contents

CHAPTER 1

INTRODUCTION TO DATA SECURITY

Chapter 1 Introduction to Data Security

1.Data Management

Data management is a critical aspect of modern organizations, as it helps organizations make better decisions and improve their operations. A data management framework is a set of guidelines, policies, and procedures that organizations use to manage their data. A data management framework typically includes processes for **data governance, data quality, data integration, and data security.**

1.1 Data Management Framework

A data management framework is a set of guidelines, policies, and procedures that organizations use to manage their data. It helps organizations ensure that their data is accurate, consistent, and reliable, so that it can be used to drive business decisions. A data management framework typically includes the following elements: data governance, data quality, data integration, data security, data privacy, data retention, data architecture, and data analytics.

1.2 Elements of a Data Management Framework

A data management framework typically includes the following elements.

1- Data governance: Data Governance is a discipline which provides the necessary policies, processes, standards, roles, and responsibilities needed to ensure that data is managed as an asset.

Data governance adds meaning and security to an organization's data by allowing teams to organize, record, and assess the quality of existing information assets. Data governance ensures that all colleagues have the context they need to trust data, access data, and produce important insights by defining terminology, setting policies, assigning duties, and more.

2- Data quality: Data quality is the process of ensuring that the data is accurate, complete, and consistent. This includes processes for data validation, data cleansing, and data matching, as well as data quality metrics and data quality reporting.

3- Data integration: Data integration is the process of integrating data from different systems and applications. This includes processes for mapping data elements, data transformation, and data cleansing, as well as data integration tools and data integration best practices.

4- Data retention: Data retention is the process of storing data for a certain period, as per legal, regulatory and/or business requirements. It includes data archiving, data purging and data retention policies.

5- Data architecture: Data architecture is the process of designing the data models and database structures that support the organization's business requirements. This includes data modeling, database design, and data architecture best practices.

6- Data analytics: Data analytics is the process of analyzing data to extract insights and make better decisions. This

includes data warehousing, data mining, and data visualization.

7- Data security: Data security is the process of protecting data from unauthorized access, use, disclosure, disruption, modification, or destruction. This includes data encryption, data access controls, and data security best practices.

1.3 Data Security

Data Security Definition

Data security is a set of standards and technologies that protect data from intentional or accidental destruction, modification, or disclosure. Data security can be applied using a range of techniques and technologies, including administrative controls, physical security, logical controls, organizational standards, and other safeguarding techniques that limit access to unauthorized or malicious users or processes.

Data and information Security comprises the three most important pillars of a security strategy. It is crucial to consider the security elements when considering how to protect our data and considered as a benchmark model in information security that is designed to govern and evaluate how an organization handles data when it is stored, transmitted, or processed.

The security elements refer to an information security model made up of three main components: confidentiality, integrity, and availability. Each component represents a fundamental objective of information security.

Data breaches, which occur when data is accessed in an unauthorized manner, are a major concern for organizations of all shapes, sizes, and industries. So let us know what these breaches or hazards are.

1.4 Recent Security hazards

Security hazards are a harmful and intentional attempt made by a person or organization to gain access to another person's or organization's information system. Typically, the hazarder wants to gain something by crashing the victim's network.

It refers to the sets of actions that the menace actors perform to gain any unauthorized access, cause damage to systems/computers, steal data, or compromise the computer networks. A hazarder can launch a cyber-hazard from any location. The hazarder can also be an individual or even a group. There are various TTP (tactics, techniques, and procedures) to do so.

A vulnerable application could subject people and systems to several kinds of harm. A hazard occurs when an hazarder

takes advantage of security flaws or vulnerabilities to harm others.

Predicting security hazards is a complex task, as hazarders are continually refining their techniques and exploiting vulnerabilities in innovative ways. However, experts in the field closely monitor trends and analyze past hazard patterns to make informed predictions about future menace. These predictions serve as valuable insights for individuals, organizations, and security professionals who aim to enhance their defensive strategies and mitigate the risks associated with cyber-hazards.

As we delve into the predictions for cyber security hazards in 2024, it is important to note that they should be viewed as potential scenarios rather than definitive certainties. Nonetheless, understanding these predictions can help us identify potential vulnerabilities and take proactive measures to strengthen our defenses. In the following sections, we will explore some of the anticipated cyber security hazards and their potential impact in 2024. By examining these predictions, we can gain a deeper understanding of the evolving menace landscape and the steps required to ensure robust cybersecurity practices.

1.4.1 Challenges of new technologies

The evolution of cyber security menace has been a constant battle between hazarders and defenders. Over the years, we have witnessed a significant shift in the tactics and techniques employed by malicious actors. Initially, cyber-hazards were primarily focused on disrupting computer systems and causing inconvenience. However, **as technology advanced and the digital realm became more interconnected, cyber criminals began targeting sensitive data and financial assets.**

One of the key factors driving the evolution of cyber security menace is **the increasing sophistication of hazarders**. Hackers are continually refining their techniques, leveraging advanced tools and technologies to exploit vulnerabilities in software, networks, and human behavior. They exploit weaknesses in outdated software, misconfigured systems, and unsuspecting individuals to gain unauthorized access to sensitive information.

Another significant aspect of the evolution of cyber security menace is **the rise of nation-state sponsored hazards**.

State-sponsored hacking activities have become more prevalent, with governments and intelligence agencies deploying cyber-hazards, these hazards often target critical infrastructure, government institutions, and high-value targets, posing a significant menace to national security.

Additionally, the advent of emerging technologies has introduced new avenues for cyber-hazards.

The widespread adoption of the Internet of Things (IoT), cloud computing, artificial intelligence (AI), and blockchain has opened new hazard vectors and vulnerabilities. Hazarders can exploit insecure IoT devices, compromise cloud-based services, manipulate AI algorithms, and launch crypto-jacking hazards to mine cryptocurrencies surreptitiously.

The evolution of cyber security menace is also closely tied to the growing interconnectedness of our digital lives. As more devices, systems, and individuals become interconnected, the hazard surface expands, offering hazarders a broader range of targets. The increasing reliance on digital infrastructure for critical functions such as healthcare, transportation, and finance make these sectors particularly vulnerable to cyber-hazards.

To effectively combat the evolving cyber security menace, organizations and individuals must stay vigilant and adapt their defenses accordingly. Proactive measures such as regular software updates, strong authentication protocols, employee training, and robust incident response plans are essential to mitigate the risks posed by this menace. Furthermore, collaboration between governments, industry

stakeholders, and security professionals is crucial to share menace intelligence, develop effective defense strategies, and stay one step ahead of cyber criminals.

1.4.2 Emerging Technologies and Flaws:

The rapid advancement of emerging technologies has undoubtedly brought numerous benefits to society, but it has also introduced a range of vulnerabilities that cybercriminals can exploit. Understanding these vulnerabilities is crucial for effective cyber security. **Let's explore some of the key emerging technologies and the associated risks they pose.**

1. **Internet of Things (IoT):** The proliferation of IoT devices has created a vast network of interconnected smart devices, ranging from household appliances to industrial sensors. While the IoT offers convenience and efficiency, it also presents significant security challenges. Many IoT devices have weak security protocols, making them easy targets for hazarders. Compromised IoT devices can be used to launch large-scale distributed denial-of-service (DDoS) hazards or gain unauthorized access to networks.
2. **Artificial Intelligence (AI)**: AI technologies are increasingly being utilized in various applications, including cybersecurity. While AI can enhance

menace detection and response capabilities, it can also be exploited by hazarders. Adversarial machine learning techniques can be used to deceive AI systems, leading to false positives or false negatives in menace detection. Additionally, AI-powered social engineering hazards can manipulate human behavior and deceive individuals into divulging sensitive information.

3. **Blockchain:** Blockchain technology, known for its decentralized and tamper-resistant nature, has gained significant attention in recent years. However, even though blockchain itself is considered secure, vulnerabilities can arise in the surrounding infrastructure. Smart contract vulnerabilities, flaws in wallet software, and social engineering hazards targeting cryptocurrency users are some of the risks associated with blockchain technology.
4. **5G Networks:** The rollout of 5G networks promises increased speed, bandwidth, and connectivity. However, it also expands the hazard surface. With more devices connected to high-speed networks, the potential for large-scale hazards increases. Additionally, the reliance on virtualized network

infrastructure introduces new vulnerabilities that hackers can exploit.

To address emerging technology vulnerabilities, a multi-faceted approach is required. First and foremost, security needs to be integrated into the design and development of these technologies from the outset. This includes implementing strong encryption, authentication mechanisms, and regular security updates.

Furthermore, organizations and individuals must stay updated on emerging menace and best practices through continuous education and training programs. Collaboration among technology vendors, security researchers, and policymakers is essential to identifying vulnerabilities, sharing menace intelligence, and developing effective security measures.

Governments also play a crucial role in ensuring a secure digital environment by establishing regulations and standards that promote security and privacy in emerging technologies. This includes incentivizing secure development practices, encouraging responsible disclosure of vulnerabilities, and holding manufacturers accountable for the security of their products.

1.4.3 Predicted Security hazards expected in 2024.

As we look ahead to the year 2024, several security trends are expected to shape the menace landscape. These trends highlight the evolving tactics of cybercriminals, and the challenges organizations will face in safeguarding their digital assets. Here are some predicted trends for 2024:

1. **increased Sophistication of Ransomware:** Ransomware hazards have been on the rise in recent years, and they are expected to become even more sophisticated in 2024. Cybercriminals will likely employ advanced techniques such as machine learning and artificial intelligence to improve the efficiency and effectiveness of their hazards. Additionally, ransomware hazards targeting critical infrastructure, healthcare systems, and government organizations are likely to escalate, causing significant disruptions and financial losses.
2. **Targeting of Internet of Things (IoT) Devices:** With the proliferation of IoT devices, cybercriminals will increasingly focus on exploiting their vulnerabilities. IoT devices often have weak security measures, making them attractive targets for hackers. We can expect hazards targeting smart homes, connected cars, and industrial IoT systems to become more prevalent.

Compromised IoT devices can be used for data theft, botnets, or even physical damage in critical sectors.

3. **Advanced Persistent Menace (APTs):** APTs are highly sophisticated, targeted hazards that aim to gain long-term unauthorized access to systems. In 2024, APTs are predicted to become more widespread and stealthier, posing significant challenges for organizations. Hazarders will employ advanced evasion techniques, such as living-off-the-land (LotL) hazards, where they utilize legitimate tools and processes to bypass security controls. APTs will likely focus on high-value targets like government agencies, financial institutions, and large corporations.
4. **Mobile Device Exploitation:** Mobile devices have become an integral part of our lives, making them attractive targets for cybercriminals. In 2024, we can expect an increase in mobile-specific menaces, including mobile malware, banking trojans, and phishing hazards targeting mobile users. As mobile devices store a wealth of personal and financial information, their compromise can lead to identity theft, financial fraud, and unauthorized access to sensitive data.

5. **Emphasis on Privacy and Data Protection:** With the growing concerns surrounding data privacy, regulatory frameworks such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) will continue to influence the cyber security landscape in 2024. Organizations will need to prioritize privacy and implement robust data protection measures to comply with these regulations. Additionally, consumers will demand greater transparency and control over their personal data, prompting businesses to adopt more secure data handling practices.
6. **Artificial Intelligence in Cyber Hazards and Defense:** Both hazarders and defenders will increasingly leverage artificial intelligence (AI) in their strategies. Hazarders will use AI to automate hazards, improve evasion techniques, and enhance social engineering tactics. On the other hand, organizations will employ AI-powered security solutions to detect and respond to menace in real-time. AI will play a pivotal role in menace intelligence, anomaly detection, and incident response, shaping the future of cyber security operations.

Chapter 1- Introduction to Data Security

1.5 The Roles of security Measures:

Cybersecurity measures play a critical role in safeguarding digital systems, networks, and data from unauthorized access, manipulation, and disruption. In the context of evolving cyber menace, the role of cybersecurity measures becomes even more vital. **Here are some key aspects of cybersecurity measures and their significance:**

Role 1: The primary goal of cybersecurity measures is to prevent cyber-hazards from occurring in the first place. This involves implementing robust security controls, such as firewalls, intrusion detection and prevention systems, secure network architecture, and strong access controls. By establishing multiple layers of protection, organizations can significantly reduce the risk of successful cyber-hazards.

Role 2: Despite preventive measures, it's essential to assume that some hazards may still penetrate the defenses. Detection mechanisms, such as security monitoring tools, log analysis, and menace intelligence, play a crucial role in identifying and alerting organizations about potential security incidents. Rapid detection enables prompt response and mitigates the impact of cyber-hazards.

Role 3: Cybersecurity measures encompass well-defined incident response procedures. These procedures outline the steps to be taken when a security incident occurs, including containment, investigation, mitigation, and recovery. Incident response teams, comprising IT professionals, legal experts, and communication specialists, collaborate to minimize the damage caused by an hazard and restore normal operations.

Role 4: Regular vulnerability assessments and penetration examination are crucial components of cybersecurity measures. They help identify and address weaknesses in systems, applications, and network infrastructure. By proactively patching vulnerabilities and implementing security updates, organizations reduce the hazard surface and mitigate the risk of exploitation.

Role 5: Human factors remain a significant source of cyber vulnerabilities. Effective cybersecurity measures include comprehensive user awareness and training programs to educate employees about best practices, social engineering menace, phishing hazards, and the importance of strong passwords. Empowering users to recognize and respond

appropriately to potential menace enhances the overall security posture of an organization.

Role 6: Protecting sensitive data is a key aspect of cybersecurity measures. Encryption techniques are employed to secure data both at rest and in transit. Encryption ensures that even if an hazarder gains unauthorized access to the data, it remains unreadable without the decryption keys. Additionally, data backup strategies and disaster recovery plans are essential to protect against data loss and facilitate business continuity.

Role 7: Cybersecurity measures also encompass compliance with industry-specific regulations and data protection laws. Organizations must ensure they meet the necessary legal and regulatory requirements related to privacy, data handling, and security. This may involve implementing specific controls, conducting audits, and maintaining documentation to demonstrate compliance.

Role 8: Cybersecurity measures are not a one-time implementation but an ongoing process. Continuous monitoring of systems, networks, and user activities helps detect anomalies and potential security breaches. Regular security assessments, audits, and

updates based on emerging menace and best practices ensure that the cybersecurity measures remain effective and up to date.

1.5.1 Collaboration and Information Sharing:

Collaboration and information sharing are crucial aspects of effective cybersecurity measures. In the face of increasingly sophisticated cyber menace, no organization can afford to operate in isolation. Here are some key points highlighting the importance of collaboration and information sharing in cybersecurity:

1. **Menace Intelligence Sharing:** Cybersecurity menaces are dynamic and constantly evolving. By sharing information about new and emerging menaces, organizations can collectively enhance their defenses. Menace intelligence sharing involves the exchange of data, indicators of compromise (IOCs), hazard patterns, and other relevant information among trusted entities. This enables organizations to proactively update their security measures and protect against known menace.
2. **Industry Collaboration:** Collaboration within industries, sectors, and communities is vital to

combating cyber menace effectively. Sharing insights, best practices, and lessons learned among peers helps raise the overall security posture. Industry collaborations often involve establishing information sharing forums, working groups, or committees that focus on specific cyber menace areas. These collaborative efforts promote collective defense and foster a culture of cybersecurity across the industry.

3. **Public-Private Partnerships:** Governments, regulatory bodies, and law enforcement agencies play a crucial role in cybersecurity. Public-private partnerships facilitate cooperation between public entities and private organizations to address cyber menace. Such collaborations involve sharing menace intelligence, coordinating incident response efforts, and working together to develop cybersecurity policies and regulations. By pooling resources and expertise, public-private partnerships strengthen the overall cybersecurity ecosystem.
4. **Information Sharing Platforms:** Dedicated platforms and forums exist for organizations to share information and collaborate on cybersecurity matters. These platforms facilitate the exchange of menace

intelligence, incident reports, and best practices among trusted members. Examples include computer emergency response teams (CERTs), information sharing and analysis centers (ISACs), and sector-specific forums. Participation in these platforms enables organizations to gain valuable insights and stay updated on the examination menace.

5. **Incident Response Collaboration:** When a cyber hazard occurs, timely and effective incident response is critical. Collaboration between affected organizations, incident response teams, and relevant stakeholders is essential to contain the incident, mitigate the damage, and restore normal operations. Sharing information about the hazard, indicators of compromise, and remediation strategies helps other organizations fortify their defenses and prevent similar incidents.

6. **International Cooperation:** Cyber menace are not limited by geographical boundaries. International cooperation and collaboration are crucial to addressing cybercrime, state-sponsored hazards, and global cyber menace. Governments, international organizations, and cybersecurity agencies work

together to share intelligence, coordinate investigations, and develop policies and frameworks to combat cyber menace at a global level.

7. **Ethical Hacking and Bug Bounty Programs:** Organizations often leverage the expertise of ethical hackers to identify vulnerabilities in their systems. Bug bounty programs encourage security researchers to responsibly disclose vulnerabilities in exchange for rewards. Collaboration with ethical hackers and bug bounty programs helps organizations discover and address vulnerabilities before malicious actors exploit them.

1.6 Elements for launching Cyber hazards.

Launching cyber hazards on information systems, computer systems, and networks in which information is stored and transmitted has three elements: motivation, technique, and vulnerabilities.

1. **motivation**

Whoever hazards information systems has the motivation to do this because of **money**, **The desire for revenge**, or the **desire to attract many customers** (as in the case of competing companies).

2.**tcchniquc**

The hazarder will not be able to launch a successful hazard if he does not have a good plan. There should be a clear hazard method to achieve the purpose. This is what differentiates between professional hazarders and non-professionals.

To repel these hazards or mitigate the damage, we must have knowledge of hazard methods and plans and the requirements for successful implementation.

3.**System Weakness**

Weaknesses in the system's setup or architecture are referred to as vulnerabilities. Cybercriminals may use a weakness to breach a security measure and access a computer system without authorization. A cyber hazard can run harmful code, set up malware, and even steal sensitive data after exploiting a vulnerability.

What causes system weakness?

There are many causes of system weaknesses, including:

- **Complexity:** Complex systems increase the probability of a flaw, misconfiguration, or unintended access.

- **Familiarity:** Common code, software, operating systems, and hardware increase the probability that a

hazarder can find or has information about known vulnerabilities.

- **Connectivity:** The more connected a device is, the higher the chance of vulnerability.

- **Ineffective Credential Management:** Weak credentials can be broken with brute force, and reusing credentials can result in one data breach becoming many.

- **Operating System Flaws:** Like any software, operating systems can have flaws. Operating systems that are insecure by default allow any user to gain access and potentially inject viruses and malware.

- **Internet Usage:** The Internet is full of spyware and adware that can be installed automatically on computers.

- **Software Bugs:** Programmers can accidentally or deliberately leave an exploitable bug in software. Sometimes end users fail to update their software,

leaving it unpatched and vulnerable to exploitation.

- **Unchecked User Input:** If your website or software assumes all input is safe, it may execute unintended SQL commands.

- **People:** The biggest vulnerability in any organization is the human at the end of the system. Social engineering is the biggest menace to many organizations. So, employees are the greaexamination menace to information security because They are the closest to organizational data.

1.7 Data Security Technologies

Data security technology and mechanisms come in many shapes and forms and protect data from a growing number of menace. Many of these menace are from external sources, but organizations should also focus their efforts on safeguarding their data from the inside, too. Ways of securing data include:

1.Data masking: Data masking involves obscuring data so it cannot be read. Masked data looks like the authentic data set but reveals no sensitive information. Legitimate data is replaced so the masked data maintains the characteristics of the data set as well as referential integrity across systems, thereby ensuring the data is realistic, irreversible, and repeatable.

Masking specific areas of data can protect it from disclosure to external malicious sources, and internal personnel who could potentially use the data. For example, the first 12 digits of a credit card number may be masked within a database. Below are some common data masking techniques:

- scrambling
- shuffling
- data aging
- variance
- masking out

- nullifying

Data masking is useful when certain data is needed for software examination, user training and data analysis -- but not the sensitive data itself.

While the result of encryption and masking are the same -- both create data that is unreadable if intercepted -- they are quite different.

2.Data erasure: There are times when data that is no longer active or used needs to be erased from all systems. For example, if a customer has requested for their name to be removed from a mailing list, the details should be deleted permanently.

3.Data resilience: By creating backup copies of data, organizations can recover data should it be erased or corrupted accidentally or stolen during a data breach.

CHAPTER 2

ETHICAL HACKING

Chapter 2 Ethical Hacking

2.1 Ethical hacking definition

When many people hear the term hacking, it's often correlated with cyberhazards. However, in today's technology-driven world, there's a group of cybersecurity professionals that essentially hack the hackers; they're called ethical hackers, and the process is called ethical hacking.

Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or piece of data. Carrying out an ethical hack involves duplicating the strategies and actions of malicious hazarders. This practice helps to identify security vulnerabilities, which can then be resolved before a malicious hazarder can exploit them.

2.2 Classifications of hackers

Using the term hacking or hacker usually has a negative connotation in its definition. Malicious hackers are often highly skilled in coding, programming, and modifying computer software and hardware systems to gain unauthorized access. However, not all hackers are created equal, and they're not always cybercriminals.

Hacking consists of conducting technical activities with the intent of exploiting vulnerabilities within a computer system, network, or firewall to obtain unauthorized access. It involves misusing digital devices such as computers, networks, smartphones, and tablets.

The goal of hacking is to manipulate digital devices to cause damage or corrupt operating systems. It also allows hackers to collect user information, steal sensitive information and documents, or perform other disruptive data-related activities.

While hackers can be both ethical and malicious, most fall within the three main types of hacking. These three main varieties of hackers are authorized, unauthorized and grey-hat hackers. Each type has different intents and purposes for their exploits. Let's explore each of these types of hackers and how they operate.

Unauthorized Hackers

Unauthorized hackers, also called black-hat hackers, are malicious types of hackers. These hackers often use their technical skills and knowledge to seize control of computers and operating systems with the intent of stealing valuable data. Unauthorized hackers will utilize many methods to

gain unauthorized access to computer systems and networks to steal sensitive organization or individual data.

Unauthorized hackers are often the criminals behind many significant data breaches and exploits. Most of them commonly use malware, social engineering, and denial-of-service tactics to execute hazards against organizations.

Unauthorized hackers may act on their own, as part of a larger cybercrime organization or on behalf of an enemy nation-state. Most are motivated by reputation, monetary gain, or espionage conducted against both nation-states and corporations.

Authorized Hackers

Authorized hackers, also called white-hat hackers, are what many in the information security industry call **ethical hackers**. While most unauthorized hackers do not follow laws or permissions to target systems, authorized hackers will. They are expected to follow a code of ethics while also following established laws and access permissions when conducting their activities.

Authorized hackers are generally hired directly by companies or clients to examine operating systems, hardware, software, and network vulnerabilities. They will

utilize their hacking knowledge, skills, and expertise to help companies improve their security posture from hazards.

Authorized hackers break into systems to find vulnerabilities so that companies can patch their systems and mitigate potential cyber menace. They also conduct penetration examinations as part of their role. Penetration examination will expose the weaknesses in a network and examination its security measures. It can also determine how vulnerable it is to hazards from malicious hackers.

2.2.1 key concepts of ethical hacking?

Hacking experts follow four key protocol concepts:

1. **Stay legal**. Obtain proper approval before accessing and performing a security assessment.
2. **Define the scope**. Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.
3. **Report vulnerabilities**. Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.

4. **Respect data sensitivity**. Depending on the sensitivity of the data, ethical hackers may have to agree to a non-disclosure agreement in addition to other terms and conditions required by the assessed organization.

Grey-Hat Hackers

Aside from the authorized and unauthorized hackers, there is another type of hacker that is a blend of both. These types of hackers are commonly called grey-hat hackers. Grey-hat hackers are individuals who exploit security vulnerabilities to spread public awareness that the vulnerability exists. While these hackers do not share the malicious intent commonly attributed to unauthorized hackers, they also don't necessarily adhere to a code of ethics like authorized hackers.

Grey-hat hackers may opt to reveal the security vulnerability privately to the company or manufacturer without publicizing the results. However, many grey-hat hackers will publicly exploit the vulnerability found in hardware or software programs without manufacturer permission to raise awareness of the problem.

A common concern within the cybersecurity industry is that when a grey hat releases an exploit, it makes it easier for malicious hackers to steal information and data from systems.

For instance, a group of grey-hat hackers identified and released a security gap in several models of Linux routers. This release resulted in updates for companies and individuals, allowing for the closing of that security gap. However, the exposure may have also resulted in many hazards on individuals and organizations because the exploit was released publicly.

2.2.2 Ethical hackers vs. Malicious hackers

Ethical hackers use their knowledge to secure and improve the technology of organizations. They provide an essential service to these organizations by looking for vulnerabilities that can lead to a security breach.

The ethical hacker reports the identified vulnerabilities to the organization. Additionally, they provide remediation advice. In many cases, with the organization's consent, the ethical hacker performs a re-examination to ensure the vulnerabilities are fully resolved.

Malicious hackers' "Crackers" intend to gain unauthorized access to a resource (the more sensitive, the better) for financial gain or personal recognition. Some malicious hackers deface websites or crash backend servers for fun, reputation damage, or financial loss. The methods used and vulnerabilities found remain unreported. They aren't concerned with improving the organization's security posture.

The following table shows the difference between the" authorized" hackers and the "unauthorized" crackers according to different parameters.

Parameters	Ethical Hackers	Malicious Hackers
Definition	Hackers are good people who hack devices and systems with good intentions. They might hack a system for a specified purpose or for obtaining more knowledge out of it.	Malicious hackers (crackers) are people who hack into a system by breaking into it and violating it with some bad intentions. They may hack a system remotely for stealing the contained data or for harming it permanently.

Skills and Knowledge	They have advanced knowledge of programming languages and computer OS. Hackers are very skilled and intelligent people.	These people may be skilled. But most of the time, they don't even need extensive skills. Some crackers only have a knowledge of a few illegal tricks that help them in stealing data.
Role in an Organization	Hackers work with specific organizations to help them in protecting their information and important data. They mainly provide organizations with expertise in security and internet safety.	Crackers harm an organization. These are the people from whom hackers defend sensitive data and protect the organizations.
Ethics	These are ethical types of professionals.	These are illegal and unethical types of people who only focus on benefiting themselves with their hacking.
Data Security	They protect the data and never steal or damage it. Their only intention is to gain	They usually steal, delete, corrupt, or compromise the data they find from a

	knowledge from the concerned data and information.	system's loopholes. Your data stays vulnerable in the hands of a cracker.
Use of Tools	Hackers use their own legal tools for checking network strength, establishing security, and protecting an organization from internet menace.	Crackers don't have any tools of their own. They make use of someone else's tools for performing illegal activities and harming/ compromising a system.
Network Strength	They help improve a network's strength.	They harm and deplete a network's strength.
Certification	They always have legal certificates for hacking, for example, XCEH certificates. Hackers have nothing to hide and perform legal activities. Thus, they need certification for the work they do.	They usually don't have any certificates as they are unskilled. But some of them may even have certificates. Crackers usually refrain away from certification because they prefer staying anonymous about their work.

Chapter 2- Ethical Hacking

2.3 What problems does hacking identify?

While assessing the security of an organization's IT asset(s), ethical hacking aims to mimic an hazarder. In doing so, they look for hazard vectors against the target. The initial goal is to perform reconnaissance, gaining as much information as possible.

Once the ethical hacker gathers enough information, they use it to look for vulnerabilities in the asset. They perform this assessment with a combination of automated and manual examination. Even sophisticated systems may have complex countermeasure technologies that may be vulnerable.

They don't stop at uncovering vulnerabilities. Ethical hackers use exploits against the vulnerabilities to prove how a malicious hazarder could exploit them.

Some of the most common vulnerabilities discovered by ethical hackers include:

- Injection hazards
- Broken authentication
- Security misconfigurations

- Use of components with known vulnerabilities
- Sensitive data exposure

After the examination period, ethical hackers prepare a detailed report. This documentation includes steps to compromise the discovered vulnerabilities and steps to patch or mitigate them.

2.4 Limitations of ethical hacking?

- **Limited scope**. Ethical hackers cannot progress beyond a defined scope to make an hazard successful. However, it's not unreasonable to discuss out-of-scope hazard potential with the organization.
- **Resource constraints**. Malicious hackers don't have the time constraints that ethical hackers often face. Computing power and budget are additional constraints for ethical hackers.
- **Restricted methods**. Some organizations ask experts to avoid examination cases that lead the servers to crash (e.g., denial of service (DoS) hazards).

2.5 Skills and certifications should an ethical hacker obtain.

An ethical hacker should have a wide range of computer skills. They often specialize, becoming subject matter

experts (SME) in a particular area within the ethical hacking domain.

All ethical hackers should have:

- Expertise in scripting languages.
- Proficiency in operating systems
- A thorough knowledge of networking.
- A solid foundation in the principles of information security.

Some of the most well-known and acquired certifications include:

- EC Council: Certified Ethical Hacking Certification
- Offensive Security Certified Professional (OSCP) Certification
- CompTIA Security+
- Cisco's CCNA Security
- SANS GIAC

Chapter 2- Ethical Hacking

CHAPTER 3

DATABASE SECURITY

Chapter 3 Database Security

3.1 What is database security?

Database security is the processes, tools, and controls that secure and protect databases against accidental and intentional menaces. The objective of database security is to secure sensitive data and maintain the confidentiality, availability, and integrity of the database. In addition to protecting the data within the database, database security protects the database management system and associated applications, systems, physical and virtual servers, and network infrastructure.

To answer the question "what is database security," it's important to acknowledge that there are several types of security risks. Database security must guard against human error, excessive employee database privileges, hacker and insider hazards, malware, backup storage media exposure, physical damage to database servers, and vulnerable databases such as unpatched databases or those with too much data in buffers.

3.2 Types of database security

To achieve the highest degree of database security, organizations need multiple layers of data protection. To that end, a security strategy places multiple controls across the IT system. If one layer of protection fails, then another is in place to immediately prevent the hazard, as illustrated below.

- **Access control** is managed by the system administrator who assigns permissions to a user within a database. Permissions are ideally managed by adding user accounts to database roles and assigning database-level permissions to those roles. For example, row-level security (RLS) allows database administrators to restrict reading and write access to rows of data based on a user's identity, role

memberships, or query execution context. RLS centralizes the access logic within the database itself, which simplifies the application code and reduces the risk of accidental data disclosure.

Menace protection

- **Auditing** tracks database activities and helps maintain compliance with security standards by recording database events to an audit log. This allows you to monitor ongoing database activities, as well as analyze and investigate historical activity to identify potential menace or suspected abuse and security violations.
- **Menace detection** uncovers anomalous database activities that indicate a potential security menace to the database and can surface information about suspicious events directly to the administrator.

Information protection

- **Database backup data and recovery** is critical to protecting information. This process involves making backup copies of the database and log files on a regular basis and storing the copies in a secure location. The backup copy and file are available to

restore the database in the event of a security breach or failure.

- **Physical protection** strictly limits access to the physical server and hardware components. Many organizations with on-premises databases use locked rooms with restricted access for the database server hardware and networking devices. It's also important to limit access to backup media by storing it at a secure offsite location.

3.3 Why is database security important?

Organizations of every size in the public and private sectors struggle with database security challenges. Preventing data breaches is business-critical because they can lead to:

Data theft

Databases are prime targets for cyberhazards because they often store valuable, confidential, and sensitive information, including customer records, credit card numbers, bank account numbers, and personal identification numbers. Hackers use this information to steal identities and make unauthorized purchases.

Damage to business and brand reputation

Customers hesitate to do business with companies that don't protect their personal data. Database security issues that compromise customer information can damage the organization's reputation, resulting in a decline in sales and customer churn. To protect their reputation and rebuild customer trust, some businesses increase their investments in public relations, and offer credit monitoring systems to their data breach victims at no charge.

Revenue loss

A data breach can halt or slow down business operations and revenue generation until the database security challenges are resolved, the system is completely up and running again, and business continuity is restored.

Increased costs

Although the numbers vary by industry, data breaches can cost millions of dollars to fix, including legal fees, assisting victims, and extra expenses to recover data and restore systems. Companies might also pay ransomware to hackers who demand payment to restore their locked files and data. To protect against these costs, many businesses add cyber insurance to their policies.

Data breach violation penalties

State and local agencies impose fines, and in some cases require that customers are compensated, when companies don't protect their customer data.

3.4 Database security deployment

There are three layers of database security: the database level, the access level, and the perimeter level. Security at the database level occurs within the database itself, where the data live. Access layer security focuses on controlling who can access certain data or systems containing it. Security policy at the perimeter level determines who can and cannot get into databases. Each level requires unique security solutions.

Security Level	Database Security Solutions
Database Level	• Masking • Tokenization • Encryption
Access Level	• Access Control Lists • Permissions
Perimeter Level	• Firewalls

	• Virtual Private Networks

Database security best practices

Although there are several different approaches to data security, some best practices can help you keep your databases safe. These database security best practices help you to minimize your vulnerabilities while maximizing your data protection. While these approaches can be deployed individually, they work best together to protect against various circumstances impacting database security.

Physical database security

It's critical to not overlook the physical hardware where the data is stored, maintained, and manipulated. Physical security includes locking the room where the database server is — whether on-premises or accessed through the cloud. It also involves having security teams monitor physical access to that equipment.

A crucial aspect of this best practice is to have database backup and disaster recovery measures in place in case of a physical catastrophe. It's also important not to host web servers and applications on the same server as the database the organization wants to secure. As mentioned below, another consideration is to have data "encrypted at rest", so

that if a system's physical storage was stolen or compromised, the data would still be secure.

This database security measure is like access control lists and determines who can access web applications and how they can do so. There are also firewalls for individual web applications that deliver the same benefits as traditional firewalls.

Isolate sensitive databases

It's very difficult to penetrate database security if sensitive databases are isolated. Depending on how the isolation techniques are deployed, unauthorized users might not even know sensitive information exists. Software-defined perimeters are useful means of isolating sensitive databases so that they don't appear to be on a particular user's network. This approach makes it difficult to take over databases with lateral movement hazards; it's also effective against zero-day hazards. Isolation strategies are one of the best ways to solidify database security at the access level. Competitive isolation solutions combine this approach with database layer security including key management and encryption.

Change management

Change management requires outlining — ideally in advance — what procedures must take place to safeguard

databases during change. Examples of changes include mergers, acquisitions, or simply different users gaining access to various IT resources. It's necessary to document what changes will take place for secure access to databases and their applications. It's also important to identify all the applications and IT systems that'll use that database, in addition to their data flows.

Database auditing

Database auditing usually requires regularly reading the log files for databases and their applications. This information reveals who accessed which repository or app, when they accessed it, and what they did there. If there is unauthorized access to data, timely audits can help reduce the overall impact of breaches by alerting database administrators.

The quicker that organizations can react to data breaches, the more time they must notify any customers involved and limit the damage done. Database auditing provides centralized oversight for database security as a final step for protection. Comprehensive auditing also includes collecting logs that will provide additional context to database activity, such as network connections, authentication, and even metrics from host systems (Bytes In/Out, CPU & memory usage).

Contemporary security solutions

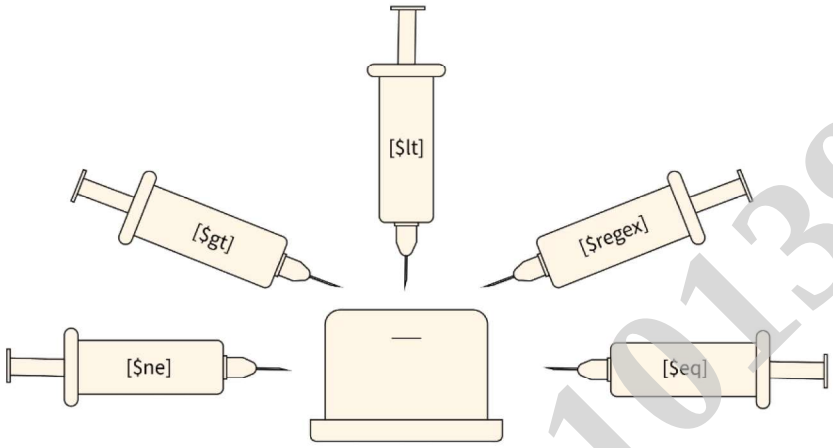
Database security is one of today's most important concerns throughout the data management landscape. You can decrease the ever-growing menace to database security by using many of the approaches described above. There are even comprehensive solutions that reinforce database security that involve many of these techniques.

Sumo Logic gives users real-time insights into their databases and applications and deploys cutting-edge Artificial Intelligence methods to add to the overall protection. Additional capabilities for troubleshooting and system monitoring make Sumo Logic the ultimate platform for fortifying database security.

3.5 Database Security Menace

Many software weaknesses, **misconfigurations**, or practices of misuse or carelessness could lead to breaches. The following are some of the most well-known causes and types of database security cyber menace.

1) SQL/NoSQL Injection Hazards



It is a type of hazard which occurs when a malicious code is injected into frontend (web) apps and then transmitted to the backend database. SQL injections provide hackers with unrestricted access to any data saved in a database. There are two types of such computer hazards: **SQL injection hazards on traditional databases** and **NoSQL injection hazards on large data databases**. Typically, these are queries generated as an extension of online application forms or received via HTTP requests. Any database system is vulnerable to these hazards if developers do not follow secure coding practices and the organization does not conduct regular vulnerability examination.

Protection measures:

- Direct queries should be replaced with stored procedures.
- The MVC Architecture must be implemented.

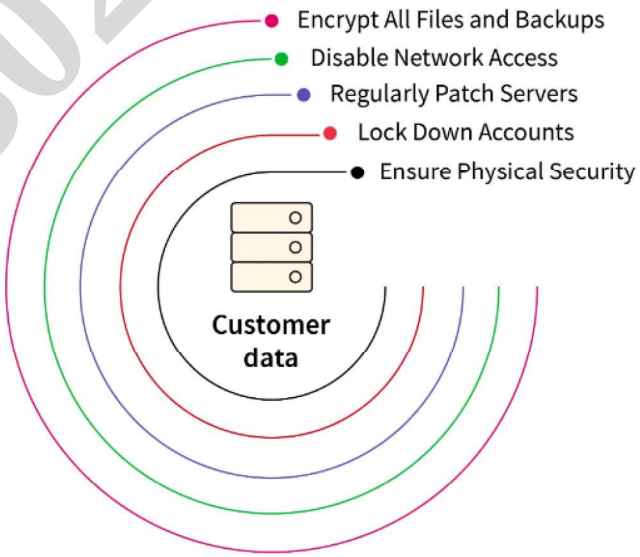
2) Lack of Security Expertise and Education

Databases are breached and leaked due to insufficient level of IT security expertise and education of non-technical employees, who may violate basic database security standards and endanger databases. IT security employees may also lack the necessary expertise to create security controls, enforce rules, or execute incident response processes.

Protection measures:

- Database users must be trained in database security.
- IT security professionals will be encouraged to advance their professional level and qualifications.

3) Exploitation of Database Software Vulnerabilities



Hazarders are continuously attempting to isolate and target software vulnerabilities, and database management software is a particularly desirable target. New **vulnerabilities** are identified on a daily basis, and security updates are issued regularly by all open-source database management platforms and commercial database software manufacturers. However, if you do not apply these changes immediately, your database may be vulnerable to hazard.

Even if you deploy patches on time, there is always the risk of **zero-day** hazards, which occur when hazarders find a vulnerability that the database vendor has not yet found and patched.

Protection measures:

- Encrypt any sensitive information in your database (s).
- Apply the necessary database controls and permissions.
- Conduct a regular search for new sensitive data in your databases. You may accomplish this very successfully with the **Periodic Data** Discovery tool and Compliance Manager, which will automatically discover and secure newly uploaded sensitive data.

4) Excessive Database Privileges

Database users in DBMS may have varying levels of access. However, users may abuse them, and the three basic categories of privilege abuse are as follows: excessive privilege abuse, legitimate privilege abuse, and unused privilege abuse. Excessive privileges always introduce unnecessary risks. According to statistics, 80% of hazards on company databases are carried out by current or former workers.

Protection measures:

- It is recommended that a strict access and privileges control policy be implemented and enforced.
- Don't give staff too many privileges and revoke outdated privileges as soon as possible.

5) Weak Audit Trail

If a database is not audited, it represents a risk of noncompliance with sensitive data protection rules at the national and international levels. All database events must be automatically logged and registered, and automatic auditing solutions must be used. Failure or unwillingness to do so represents a major risk on multiple levels.

Protection measures:

- Use automatic auditing solutions that have no impact on database performance.

3.6 Control Measures for the Security of Data in Databases

The following are the key control measures used to ensure data security in databases:

- The ability to access sensitive data is restricted from using authentication. For example, a mobile phone performs authentication by requesting a PIN, fingerprint, or face recognition. Similarly, a computer verifies a username by requesting the appropriate password.
- However, in the context of databases, authentication takes on a new dimension because it can occur at multiple levels. It can be done by the database itself, or the configuration can be adjusted to allow the operating system or another external means to authenticate users.
- **For example**, when creating a database in Microsoft's SQL Server a user must specify whether to use database authentication, operating system authentication, or both (the so-called mixed-mode authentication). Other databases that prioritize security use near-foolproof authentication methods such as fingerprint recognition and retinal scanning.

- By using various authentication technologies such as biometrics for retina and fingerprints, you can protect your data from **unauthorized/malicious** users.
- Database access control is a means of restricting access to sensitive company data to only those people **(database users)** who are authorized to access such data and permitting access to unauthorized persons. It is a key security concept that reduces risk to the business or organization.
- Physical and logical access control are the two types of access control. Access to campuses, buildings, rooms, and physical IT assets is restricted through physical access control. Connections to computer networks, system files, and data are restricted through logical access control.
- To safeguard a facility, corporations use electronic access control systems to track employee access to restricted company locations and private regions, such as data centers, using user credentials, access card readers, auditing, and reports. Some of these systems include access control panels to restrict access to

rooms and buildings, as well as alarms and lockdown features to prevent unauthorized access or operations.

- Logical access control systems execute user and entity identification, authentication, and authorization by evaluating needed login credentials, which can include passwords, personal identification numbers, biometric scans, security tokens, or other authentication factors. **Multifactor authentication** (MFA), which needs two or more authentication factors, is frequently used as part of a layered defense to safeguard access control systems.
- The most well-known Database Access Control examples are:
    - Discretionary Access Control (DAC)
    - Mandatory Access Control (MAC)
    - Role-Based Access Control (RBAC)
    - Attribute-Based Access Control (ABAC)
- Inference control in databases, also known as **Statistical Disclosure Control (SDC)**, is a discipline that aims to secure data so that it can be published without disclosing sensitive information associated with specific individuals among those to whom the data corresponds.

- It prevents the user from completing any inference channel. This strategy prevents sensitive information from indirect disclosure. There are two kinds of inferences: identity disclosure and attribute disclosure.
- SDC is used to protect the privacy of respondents in fields such as government statistics, health statistics, e-commerce **(sharing of customer data)**, etc. Since data modification ultimately implies data protection, SDC aims to achieve protection with the minimum amount of accuracy loss for database users.
- Distributed systems involve a large amount of data flow from one site to another as well as within a site. Flow control prohibits data from being transferred in such a way that unauthorized agents cannot access it.
- A flow policy specifies the channels through which data can flow. It also defines security classes for data as well as transactions. Convert channels are the pathways for information to flow implicitly in ways that violate a **company's privacy policy**.

CHAPTER 4

The importance of securing web applications

Chapter 4 The importance of securing web applications

4.1 Securing Web applications

Web application security (also known as Web AppSec) is the idea of building websites to function as expected, even when they are under hazard. The concept involves a collection of security controls engineered into a Web application to protect its assets from potentially malicious agents. Web applications, like all software, inevitably contain defects. Some of these defects constitute actual vulnerabilities that can be exploited, introducing risks to organizations. Web application security defends against such defects. It involves leveraging secure development practices and implementing security measures throughout the software development life cycle (SDLC), ensuring that design-level flaws and implementation-level bugs are addressed.

Why is web security examination important?

Web security examination aims to find security vulnerabilities in Web applications and their configuration. The primary target is the application layer (i.e., what is running on the HTTP protocol). Examination of the security of a Web application often involves sending different types of input to provoke errors and make the system behave in unexpected ways. These so called “negative examinations”

examine whether the system is doing something it isn't designed to do. It is also important to understand that Web security examinations not only about examination the security features (e.g., authentication and authorization) that may be implemented in the application. It is equally important to examine that other features are implemented in a secure way (e.g., business logic and the use of proper input validation and output encoding). The goal is to ensure that the functions exposed in the Web application are secure.

Web applications are built to store, process, and transmit sensitive data, which makes them a prime target for hackers or other malicious actors to exploit. An unsecured web application could result in losing or stealing sensitive data, downtime, or "broken" apps. The consequences include traffic reduction, lost sales, broken customer trust, or government fines under applicable laws.

4.2 pitfalls in securing web application

The most common web application security risks include the following:

- **Credential stuffing**: This hazard involves using a list of stolen credentials (usernames and passwords) to attempt to gain unauthorized access to various online accounts.

Hackers use usernames, emails, and passwords from publicly available data dumps on the dark web to take over

users' accounts. The illegal data may contain millions of usernames and password combinations due to years of data breaches on numerous sites. This shows how even old data can be valuable to hazarders.

Credential stuffing is highly dangerous, particularly in finance. Financial credential stuffing provides hackers clear access to all your bank account and transaction information, allowing them to apply for loans, use your credit cards, or conduct bank transfers.

- **SQL Injection:** This hazard involves injecting malicious code into a web application. The hazarder can do this through SQL injection or other injection hazards.

This type of flaw enables an hazarder to tamper with an application's database queries by injecting code. In most hazards, hackers can retrieve data belonging to other users or related to the application itself, such as passwords, credit card details, and cookies. When a SQL injection hazard goes awry, a hazarder may attempt a denial-of-service hazard or compromise the underlying web server or other back-end infrastructure.

- **Session hijacking:** This hazard involves taking over an active user session to gain unauthorized access to a web-

based application. Techniques included are IP spoofing, side jacking, man-in-the-middle, and session fixation.

- **Cross-site scripting (XSS):** This hazard involves injecting malicious code into a web page that gets executed by the browser of the person visiting the page.

It is a widely used technique to execute code, most commonly JavaScript, in the targeted website or application. Successful cross-site scripting grants hazarders' access to the entire application. An example of an XSS hazard is when a hacker exploits an input field's vulnerability and uses it to inject malicious code into another website. Hackers have complete control over what happens once their targets click on the infected link. The main reason why XSS is considered a high-risk security flaw is that it allows an hazarder to view data stored in Local Storage, Session Storage, or cookies on the target system. Hence, no personal data should be stored in these systems.

- **Cross-site request forgery (CSRF):** This hazard involves tricking a user into submitting a malicious request to a web application.

A CSRF hazard employs social engineering techniques to convince a user to modify application data such as the username or password. A CSRF hazard requires an application that uses session cookies solely to identify the

user making a request. These cookies are then used to track or validate user requests.

Depending on the action the user is forced to complete, the hazarder can steal money, accounts, or perform other web application hazards.

- **Sensitive data disclosure:** This is also known as data leakage or data exfiltration and can happen through a variety of channels, including email, cloud storage, social media, or through a data breach.
- **Broken authentication and session management:** This hazard exploits vulnerabilities in how a web application manages authentication and session information.
- **Security misconfiguration:** This hazard exploits configuration vulnerabilities in a web application.

Another high-risk web application vulnerability is security misconfiguration, which allows hazarders to easily take control of websites. Malicious hazarders can take advantage of a wide range of weaknesses and configuration errors, including unused pages, unpatched vulnerabilities, unsecured files and directories, and default settings.

Elements such as web and application servers, databases, or network services can all leave you open to data breaches. Hackers can manipulate any private information and take control of both user and admin accounts.

Chapter 4- The importance of securing web applications

4.3 Measures for Web Application Security

Apart from preserving the technology and features utilized in app development, web application security also establishes a high level of protection towards web servers and processes. Additionally, it safeguards web services like APIs against online menace.

The critical aspect of web application security is to ensure the applications always operate safely and smoothly. To achieve this goal, you can start with an in-depth web security examination analysis.

Web security examination means discovering and fixing all the vulnerabilities before hackers get to them. That is why it is highly recommended to carry out web application security examinations during the SDLC (Software Development Life Cycle) stages, not after the web application has been launched.

The following are some effective security strategies that can help protect web applications.

1- Conduct a Security Audit Examination

Regular website security audits are an excellent approach to ensure you're following the best practices to keep your web application secure and will quickly find any potential flaws in your systems. Not only can a security audit help you stay

on top of potential vulnerabilities for your web development company, but it also protects any business from being at risk of having hazards.

To ensure a complete and objective perspective on your security audit process, it is best to hire a professional. With their extensive experience and expertise, they'll be an asset to identify and mitigate vulnerabilities that require patch management or other fixes.

After completing a security assessment, the following step is to address all the discovered flaws. A good approach is setting priorities based on the impact level of each type of vulnerability.

Make sure to perform consistent vulnerability scans and updates. To make things more efficient, perform your web application security examination by using your vulnerability scanners to look for major injection hazards such as SQL injection, cross-site scripting, and DDoS hazards rather than scanning for all types of vulnerabilities.

In addition, remember to make sure that all servers where your web applications are hosted are up to date with the examination security patches.

2- Protect Your Data

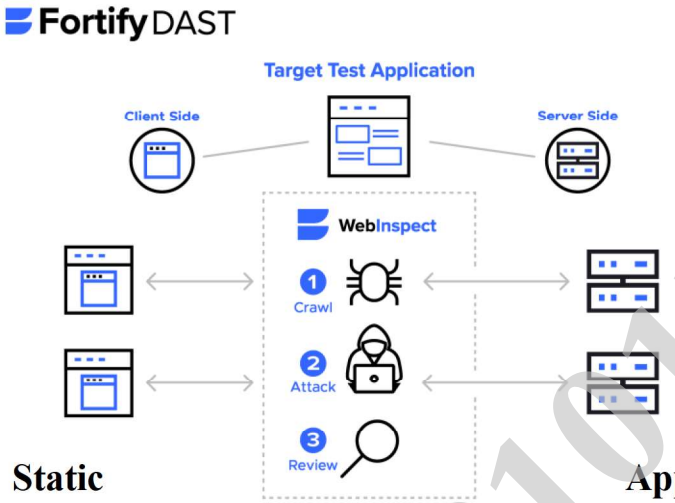
Sensitive information may be disclosed by users of online applications. No unauthorized entity should have access to

this information. Determining if your online application offers data enciphering during transit and at rest is therefore crucial. In situations like this, if your visitors use SSL or TLS, you may use HTTPS, a more secure version of the HTTP protocol.

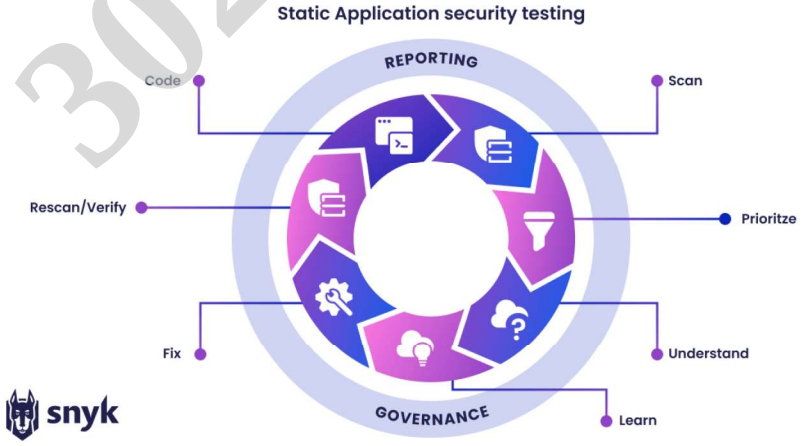
Without SSL connections, websites and applications are unsafe, which could compromise session management and the overall security system.

4.4 Different types of security examinations

- **Dynamic Application Security examination (DAST**). This automated application security examination is best for internally facing, low-risk applications that must comply with regulatory security assessments. For medium-risk applications and critical applications undergoing minor changes, combining DAST with some manual web security examination for common vulnerabilities is the best solution.



- **Static Application Security examination (SAST)**. This application security approach offers automated and manual examination techniques. It is best for identifying bugs without the need to execute applications in a production environment. It also enables developers to scan source code and systematically find and eliminate software security vulnerabilities.



- **Penetration Examination**. This manual application security examination is best for critical applications,

especially those undergoing major changes. The assessment involves business logic and adversary-based examination to discover advanced hazard scenarios.

- **Runtime Application Self Protection (RASP).** This evolving application security approach encompasses several technological techniques to instrument an application so that hazards can be monitored as they execute and, ideally, blocked in real time.

Features of the web application security examination

The following non-exhaustive list of features should be reviewed during Web application security examination. An inappropriate implementation of each could result in vulnerabilities, creating serious risk for your organization.

- Application and server configuration. Potential defects are related to encryption/cryptographic configurations, Web server configurations, etc.
- Input validation and error handling. SQL injection, cross-site scripting (XSS), and other common injection vulnerabilities are the result of poor input and output handling.

- Administration of the session and authentication. User impersonation might be caused by vulnerabilities. Credential protection and strength should also be considered.
- Privileges Examination the ability of the application to protect against vertical and horizontal privilege escalations.
- Business logic. These are important to most applications that provide business functionality.
- Client-side logic. With modern, JavaScript-heavy webpages, in addition to webpages using other types of client-side technologies (e.g., Silverlight, Flash, Java applets), this type of feature is becoming more prevalent.

A Web application in today's environment can be affected by a wide range of issues. The diagram above demonstrates several of the top hazards used by hazarders, which can result in serious damage to an individual application or the overall organization. Knowing the different hazards that make an application vulnerable, in addition to the potential outcomes of an hazard, allow your firm to preemptively address the vulnerabilities and accurately examination for them.

By identifying the root cause of the vulnerabilities, mitigating controls can be implemented during the early stages of the SDLC to prevent any issues. Additionally,

knowledge of how these hazards work can be leveraged to target known points of interest during a Web application security examination.

Recognizing the impact of an hazard is also key to managing your firm's risk, as the effects of a successful hazard can be used to gauge the vulnerability's total severity. If issues are identified during a security examination, defining their severity allows your firm to efficiently prioritize the remediation efforts. Start with critical severity issues and work towards lower impact issues to minimize risk to your firm.

Prior to an issue being identified, evaluating the potential impact against each application within your firm's application library can facilitate the prioritization of application security examining. With an established list of high-profile applications, web security examination can be scheduled to target your firm's critical applications first with more targeted examination to lower the risk against the business.

4.5 How to protect web applications?

Protecting web applications from security menace involves a combination of toolsets, services, training, staffing, and policies throughout the engineering organization.

Protecting web applications is not just left to the security organization, as many companies don't have the personnel or expertise to maintain a robust program. Modern development practices have started implementing security practices at the coding level, following it through to deployment, implementation, and maintenance after an application is released.

Organizations can take several measures to protect their web applications from security menace and minimize the risk of a data breach. However, it's important to note that no system is entirely secure, and it's essential always to be vigilant and to continuously monitor and update security measures to keep up with new menaces.

Steps organizations can take to protect their web applications:

1. Utilize a web application security solution that tracks and filters incoming traffic to a website, enabling valid traffic to get through to the origin while preventing malicious activity.

3. **Enable HTTPS:** HTTPS is a secure HTTP protocol to transmit data over the internet. Enabling HTTPS on your website or application helps to protect against data interception.

4. **Use strong, unique configurations:** You can help prevent unauthorized access by using unique, strong login credentials for all accounts connected to your website and applications.

5. **Keep software and plugins up to date:** Outdated software and plugins can contain vulnerabilities that hackers can exploit. Keeping your website's software and plugins up to date ensures you patch known vulnerabilities.

6. **Monitor and log activity**: Monitoring and logging activity on your website will help you identify suspicious activity.

7. **Regularly scan for system weaknesses:** Regularly reviewing your website and application for vulnerabilities can help you identify and address potential security issues before hazarders exploit them.

8. **Train employees:** Educating employees about security best practices can help to prevent accidental security breaches.

9. **Put security procedures in place:** Protection measures like input validation, output escaping, and error handling cut down on the hazard possibilities that hazarders can take use of.

10. **Use secure coding standards**: Have guidelines for designing and building applications and web properties.

Perform regular code reviews to identify and fix vulnerabilities before releasing code.

11. **Incident Response:** Have an incident response plan to detect and quickly respond to security breaches.

Web application security is essential to ensure web applications' safety and sensitive data and must be a priority throughout the organization. By staying informed and proactive, teams can protect their web applications and data from potential hazarders and prevent several consequences to their infrastructure, culture, and, ultimately, customer trust. An ounce of prevention is worth a pound of cure, and it's always better to take preventative measures than to clean up the aftermath of a security breach.

CHAPTER 5

ARTIFICIAL INTELLIGENCE SECURITY

Chapter 5- Artificial Intelligence Security

5.1 Artificial Intelligence Definition

Artificial intelligence (**AI**) is the ability of machines to perform tasks that are typically associated with human intelligence, such as learning and problem-solving.

Artificial intelligence is the simulation of human intelligence processes by machines, especially computer systems. Specific applications of AI include expert systems, natural language processing, speech recognition, and machine vision.

As the hype around AI has accelerated, vendors have been scrambling to promote how their products and services use it. Often, what they refer to as AI is simply a component of technology, such as machine learning. AI requires a foundation of specialized hardware and software for writing and training machine learning algorithms. No single programming language is synonymous with AI, but Python, R, Java, C++, and Julia have features popular with AI developers.

AI systems typically function by capturing enormous amounts of labelled training data, searching the data for correlations and patterns, and then utilizing these patterns to forecast future states. By studying millions of instances, an

image recognition tool may learn to recognize and describe things in photographs, much as a chatbot that is given examples of text can learn to produce lifelike dialogues with humans. Recent advances in generative AI allow us to produce realistic text, graphics, music, and other media.

AI programming focuses on cognitive skills that include the following:

- **Learning.** This aspect of AI programming focuses on acquiring data and creating rules for how to turn it into actionable information. The rules, which are called algorithms, provide computing devices with step-by-step instructions for how to complete a specific task.
- **Reasoning.** This aspect of AI programming focuses on choosing the right algorithm to reach a desired outcome.
- **Self-correction.** This aspect of AI programming is designed to continually fine-tune algorithms and ensure they provide the most accurate results possible.
- **Creativity.** This aspect of AI uses neural networks, rules-based systems, statistical methods, and other AI techniques to generate new images, new text, new music, and new ideas.

5.2 Artificial Intelligence Basics

AI refers to technologies that can understand, learn, and act based on acquired and derived information. Today, AI works in three ways:

Assisted intelligence, widely available today, improves what people and organizations are already doing.

Augmented intelligence, emerging today, enables people and organizations to do things they couldn't otherwise do.

Autonomous intelligence, which is being developed for the future, features machines that act on their own. An example of this will be self-driving vehicles when they come into widespread use.

AI can be said to possess some degree of human intelligence: a store of domain-specific knowledge; mechanisms to acquire new knowledge; and mechanisms to put that knowledge to use. Machine learning, expert systems, neural networks, and deep learning are all examples or subsets of AI technology today.

- **Machine learning** uses statistical techniques to give computer systems the ability to "learn" (e.g., progressively improve performance) using data rather than being explicitly programmed. Machine learning works best when aimed at a specific task rather than a wide-ranging mission.

- **Expert systems** are programs designed to solve problems in specialized domains. By mimicking the thinking of human experts, they solve problems and make decisions using fuzzy rules-based reasoning based on carefully curated bodies of knowledge.
- **Neural networks** use a biologically inspired programming paradigm that enables a computer to learn from observational data. In a neural network, each node assigns a weight to its input, representing how correct or incorrect it is relative to the operation being performed. The final output is then determined by the sum of these weights.
- **Deep learning** is part of a broader family of machine learning methods based on learning data representations as opposed to task-specific algorithms. Today, image recognition via deep learning is often better than humans, with a variety of applications such as autonomous vehicles, scan analyses, and medical diagnoses.

5.3 AI in security

Along with advancements in technology, cybersecurity is becoming increasingly important.

According to the FBI's Internet Crime Report 2021, the FBI's Internet Crime Complaint Centre (IC3) received 847,376 complaints of internet-related crimes. They resulted in staggering financial losses of 6.9 billion dollars, compared to 4.2 billion in 2020.

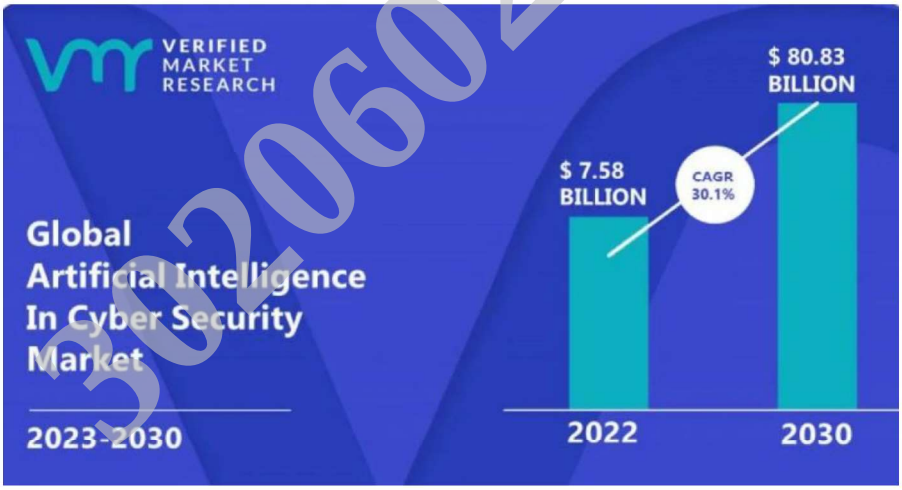
Hackers, malicious agents, or cyber hazarders constantly try to breach digital spaces. Cybercrimes such as phishing, scams, and data and identity theft are rising. To prevent these hazards, organizations employ qualified cybersecurity teams that work tirelessly to secure digital systems, leveraging new technologies, including artificial intelligence.

AI in cybersecurity analyzes system usage patterns to identify potentially malicious activities or menace actors and predict cyberhazards before they happen. AI-enabled automated monitoring protects systems 24/7 and enables organizations to take preventive measures before harm is done.

Some major AI in cybersecurity applications include:

- Malware and phishing detection
- Knowledge consolidation
- Detection and prioritizing new menace.
- Breach risk prediction
- Task automation

But before we explore these applications in detail, let's briefly look at the current state of AI in cybersecurity below.
AI in cybersecurity has been gaining traction over the past years. The idea of mitigating cybersecurity risks before they occur has been bringing in investments to develop and improve AI-powered cybersecurity systems.
The laexamination report by Verified Market Research suggests that the market size for Artificial Intelligence in cybersecurity stood at 7.58 billion dollars in 2022 and is expected to reach 80.83 billion by 2030.



AI in cybersecurity market size 2022-2030 (source)

These growing numbers are not surprising since hackers also get access to new technologies.
For instance, about 93.67% of malware observed in 2019 could modify its source, which made it nearly impossible to detect. Moreover, reportedly, 53% of consumer PCs and

50% of commercial computers were re-infected with malware after a brief recovery period.

The increasing number of cyberhazards has drawn the international community's attention towards the possible use of artificial intelligence in cybersecurity. According to a survey by The Economist Intelligence Unit, 48.9% of global executives and leading security experts believe that AI and machine learning are best equipped for countering modern cyber menace.

Moreover, a report by Pillsbury, a global law firm focusing on technology, asserted that 44% of global organizations already implement AI to detect security intrusions.

Now, let's look at some of the most significant applications of artificial intelligence in cybersecurity.

5.4 AI Applications in security

Malware and phishing detection

Malware is malicious software transferred to a user's computer (usually over a network) and designed to carry out unauthorized operations. Some common malware activities include:

- Data deletion
- Creating unnecessary copies

- Data encryption
- Accessing and controlling a device remotely
- Malicious advertising
- Monitoring user activity (spyware)

AI-based cybersecurity systems can detect malicious traits more effectively. Chuck Everette, director of cybersecurity advocacy at Deep Instinct, claims that while legacy signature-based malware detection systems effectively prevent 30% to 60% of menace, AI-powered systems have a security efficiency rate of 80% to 92%.

AI researchers and security experts employ numerous techniques. For instance, research at Plymouth University tackled malware detection using computer vision. They used binary visualization analysis to convert files into colored image representations showing a clear color distinction between malicious and benign files.

Using neural networks, the researchers achieved an overall malware detection accuracy of 74% on all file formats, with as much as 91.7% and 94.1% accuracy for .doc and .pdf files.

AI- Phishing hazards early detection

AI-based systems can detect whether a website or email is a phishing trap. Researchers from the University of North Dakota proposed a phishing detection technique based

on machine learning that analyzes the structure of emails and classifies them as legitimate or phishing emails. Using 4000 training samples, the researchers achieved an accuracy of 94%.

Another example of an effective AI-enabled phishing detection tool is Mimecasts's CyberGraph, which uses machine learning to prevent impersonation or phishing hazards. It includes three major capabilities:

- **Blocking** trackers embedded into emails that can disclose confidential information.
- **Identifying** patterns using identity graphs to detect phishing emails.
- **Alerting** users with dynamic color-coded warning banners that signify menace level.

Another prominent leader in the cyber security domain is Cofense, which has acquired Cyberfish, a provider of AI systems for phishing protection. Their combined knowledge of machine learning, computer vision, detection, and response create a real-time protection system.

Artificial intelligence can also analyze malware based on its inherent characteristics, e.g., if the software is designed to delete or encrypt files without authorization, it is most likely a menace.

Knowledge consolidation

Chapter 5- Artificial Intelligence security

Any online system is vulnerable to cybersecurity menace. Preventing them requires implementing and complying with hundreds of security protocols and standards.

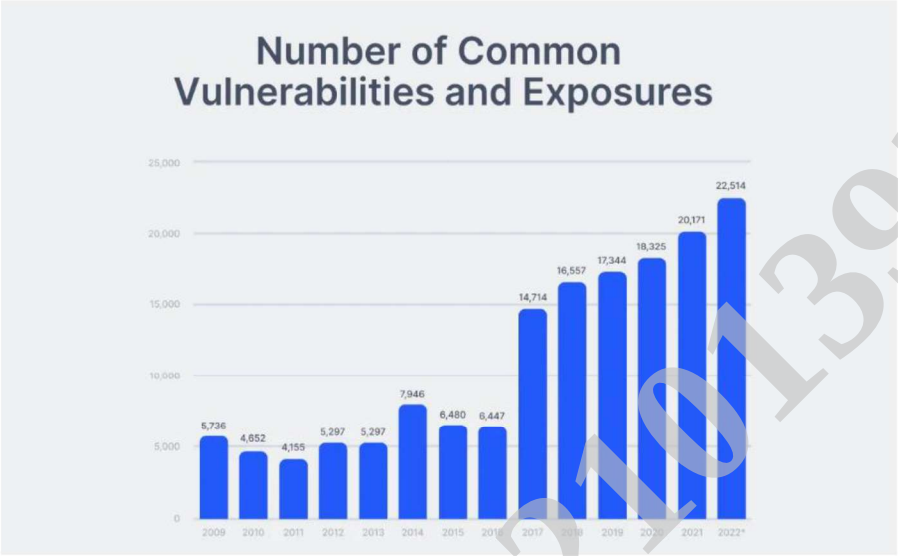
Cybersecurity professionals cannot keep up with the thousands of existing software vulnerabilities, which is why manual menace detection always carries the risk of security leaks.

Fortunately, **ML-enabled security systems can help minimize human error.** Machine learning models can retain information from decades-old data and use the consolidated knowledge to detect security breaches.

A prime example of consolidated learning is the IBM Watson platform. IBM security teams have constantly promoted Watson for advanced cybersecurity provisions. Its menace detection model is trained on millions of data points, and the cognitive learning capabilities combine computer and human intelligence for automating menace detection and reducing security incidents.

Detecting and prioritizing new menace

With the growing complexity of software architectures, the possibility of new vulnerabilities also increases. According to Statista, over 22,000 new vulnerabilities were registered in 2022 alone, the highest reported figure since 2009.



Software vulnerabilities per year 2009—2022 (source)

As mentioned above, cybersecurity professionals can't keep up with all the possible digital menace. However, machine-learning-based cybersecurity systems can keep track of all global and industry-specific vulnerabilities. AI models are constantly updated with data on the examination menace and vulnerabilities, which helps them defend against new menace actors and prevent upcoming hazards.

The success of AI in cybersecurity has encouraged tech giants such as Google, IBM, and Microsoft to develop advanced AI systems for menace identification and mitigation. In 2021, Google committed to spending $10 billion over the next five years to advance cybersecurity through various programs. Their Project Zero team finds and fixes web vulnerabilities to make the internet safer.

Moreover, Google Play Protect regularly scans over 100 billion apps for malware and other cyber menace.

Microsoft's Cyber Signals program uses AI to analyze 24 trillion security signals, 40 nation-state groups, and 140 hacker groups to detect malicious activity and software-related weaknesses. According to Microsoft's report, the Cyber Signals program blocked over 35.7 billion phishing hazards and 25.6 billion identity theft attempts on enterprise accounts.

Breach risk prediction

Large enterprises have an extensive IT asset inventory, and analyzing every component for security breach risk is complex. AI tools can identify the components most susceptible to a breach and even predict the expected hazard types.

Researchers have proposed cognitive learning-based models that monitor security access points for authorized logins. The model can detect remote hacks early, alert users, and create additional security layers to prevent a possible data breach.

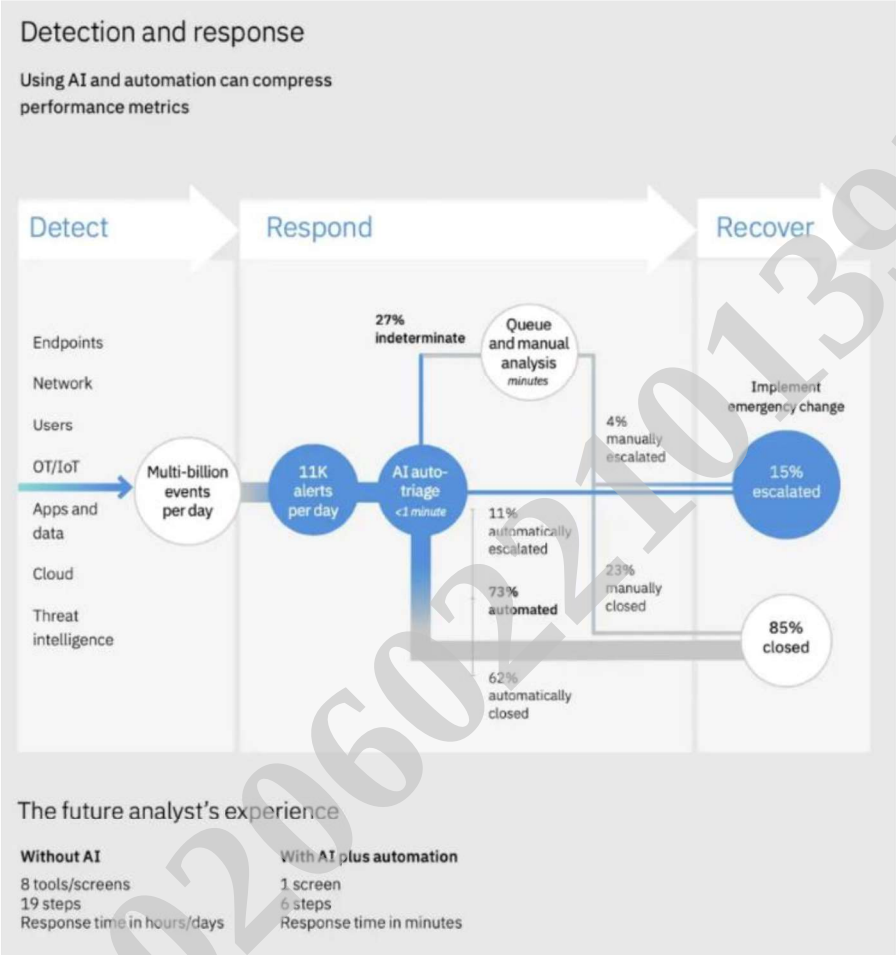
Early information on hacks and breaches can help organizations allocate resources and tools more effectively to prepare for future hazards and develop significant cyber resilience.

Chapter 5- Artificial Intelligence security

Task automation

When dealing with cyber menace, every second counts. The longer the countermeasures take, the more damage is done. A manual menace detection and mitigation process gives an hazarder ample time to encrypt or steal data, cover up their tracks, and leave backdoors inside your system.

AI can automate menace detection and take the necessary measures immediately. According to IBM, using AI methodologies, the time taken to detect and act against cyber menace can be reduced by 14 weeks.



Architecture for AI-based automated menace detection and action engine (source)

As shown above, an AI-enabled automated menace detection solution can process billions of network requests, endpoints, users, and data points daily. All these events are processed in real time to provide instant analysis and take immediate action within minutes, compared to hours or days consumed due to manual menace detection.

Chapter 5- Artificial Intelligence security

5.5 AI in security: risks and challenges

Machine learning systems have done wonders for modern-day businesses by providing critical insights, aiding decision-making, and automating cumbersome everyday tasks. However, there are still many risks and challenges that need to be taken into consideration. Gaurav Keerthi, Deputy Chief Executive Officer at the Cyber Security Agency of Singapore, says that **"AI holds great promise to provide solutions for mankind, yet from a cybersecurity perspective, AI can be both a blessing and a curse."**

Integrating AI into cybersecurity systems poses several challenges, such as:

Data manipulation. AI systems use data to understand historical patterns. Hackers can gain access to the training data, alter it to include biases, and damage the efficiency of the models. Furthermore, data can be altered to benefit the hacker more.

AI-powered cyber-hazards: Hackers can use AI techniques to develop intelligent malware that can modify itself to avoid detection by even the most advanced cybersecurity software.

Data unavailability: The performance of AI models depends on the volume and quality of data. If sufficient high-quality training data is not provided or the data contains bias issues, the AI system will not be as accurate as expected.

Based on this data, an inadequately trained model will result in false positives and a false sense of security. Any menace will go undetected and lead to substantial losses.

Privacy concerns: To properly understand user patterns, AI models are fed real-world user data. Without adequate sensitive data masking or encryption, user data is prone to privacy and security issues, favoring malicious actors.

Hazards on the AI systems: AI systems, like any other software product, are susceptible to cyberhazards. Hackers can feed these models poisonous data to alter their behavior according to their desired malicious intent.

However, all innovations are accompanied by concerns and skepticism. The right way forward is to build infrastructures that counter these risks as much as possible and provide a safe and secure environment for modern digital systems.

CHAPTER 6

INTERNET OF THINGS AND SECURITY

Chapter 6 Internet of Things and Security

6.1 Internet of Things

The internet of things, or IoT, is a network of interrelated devices that connect and exchange data with other IoT devices and the cloud. IoT devices are typically embedded with technology such as sensors and software and can include mechanical and digital machines and consumer objects.

Increasingly, organizations in a variety of industries are using IoT to operate more efficiently, deliver enhanced customer service, improve decision-making, and increase the value of their businesses.

With IoT, data is transferable over a network without requiring human-to-human or human-to-computer interactions.

A *thing* on the internet of things can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low, or any other natural or man-made object that can be assigned an Internet Protocol address and is able to transfer data over a network.

An IoT ecosystem consists of web-enabled smart devices that use embedded systems, such as processors, sensors, and communication hardware, to collect, send, and act on data they acquire from their environments.

6.2 Internet of things security

IoT cyber security is a technology segment devoted to protecting linked devices and networks on the Internet of things (IoT). IoT entails connecting a system of interconnected computing devices, mechanical and digital machinery, items, animals, and/or people to the Internet. Each "thing" is given a unique identifier and the capacity to transport data autonomously across a network. Allowing devices to connect to the Internet exposes them to several major risks if not adequately secured.

IoT security management:

- Improves security with hardware.
- Enable secure communication to sensors.
- End to End Security from Sensor to Cloud.

The Internet of Things (IoT) connects various objects and devices via the internet to communicate with similarly

connected devices or machines. With an internet connection, consumers can now purchase a wide range of products, from automobiles to refrigerators. By extending networking capabilities to all aspects of our lives, we can become more efficient, save time and money, and have access to our digital lives whenever we need it.

Cybersecurity professionals frequently refer to this fact as **increasing the hazard surface that hackers can exploit**. Security professionals are aware of this and work to manage the resulting security risks.

6.3 Why is IoT (Internet of Things) security required?

Securing IoT devices is difficult for a variety of reasons. As manufacturers and innovators are pressed to release new products, security is frequently given a lower priority than time-to-market metrics. Many businesses are also unaware of the vulnerabilities that IoT presents and are frequently more concerned with the cost savings and convenience that IoT provides.

For industrial IoT systems, the stakes are especially high. Connected IoT sensors and devices can significantly increase operational risks in everything from national power

generation and distribution infrastructures to global manufacturing operations.

In addition to securing individual IoT devices, organizations must also ensure the security of their IoT networks. Strong user authentication and access control mechanisms can help to ensure that only authorized users have access to the IoT framework.

The Internet of Things (IoT) can provide significant benefits to businesses. However, more IoT devices and a more complex IoT ecosystem mean more security vulnerabilities from the edge to the cloud. Unfortunately, many businesses continue to put off implementing an IoT cybersecurity strategy and fail to recognize IoT security risks until it is too late.

And COVID-19 has only heightened the dangers. Developing a thorough understanding of IoT cybersecurity issues and implementing a risk-mitigation strategy will help protect your business and boost confidence in digital transformation processes.

6.4 How do IoT hazards occur?

The Open Web Application Security Project (OWASP) has published a detailed draft list of IoT hazard surface areas, or areas in IoT systems and applications where menace and vulnerabilities may exist, as part of its Internet of Things Project.

The following is a summary of the IoT hazard surface areas:

1. Devices

Devices can be the primary means of launching hazards. Memory, firmware, the physical interface, the web interface, and network services are all areas where vulnerabilities can occur. Hazarders can also exploit insecure default settings, obsolete components, and insecure update mechanisms, among other things.

2. Channels of communication

Hazards on IoT devices can originate in the communication channels that connect IoT components. Protocols used in IoT systems may have security flaws that have a ripple effect on the entire system. IoT systems are also vulnerable to well-known network hazards such as DoS and spoofing.

3. Software and applications

Vulnerabilities in web applications and related software for Internet of Things devices can compromise systems. Web applications, for example, can be used to steal user credentials or distribute malicious firmware updates.

6.5 Examples of IoT Cyber Security Breaches

1. Stuxnet

Stuxnet is a sophisticated computer worm designed to detect specific nuclear machinery. Stuxnet is a computer worm that destroys real-world devices rather than hacking them to cause software damage. To infect the Windows PCs in the Natanz facility, Stuxnet exploited no fewer than four zero-day bugs: a Windows shortcut flaw, a bug in the print spooler, and two escalations of privilege vulnerabilities, along with a zero-day flaw in the Siemens PLCs and an old hole already used in the Conficker hazard. The sheer number of vulnerabilities exploited is unusual, as typically zero-days are quickly patched in the wake of a hazard, so a hacker won't want to reveal so many in a single hazard.

2. Mirai

Mirai searches the Internet for IoT devices that use the ARC processor. This CPU runs a simplified version of the Linux operating system. Mirai can infect a device if the default username and password are not changed.

IoT, or the Internet of Things, is a fancy word for smart gadgets that can connect to the Internet. These gadgets can be baby monitors, automobiles, network routers, agricultural devices, medical devices, environmental monitoring devices, home appliances, DVRs, CC cameras, headsets, or smoke detectors. To bring Dyn down, the Mirai botnet hacked 100,000 IoT devices.

3.Jeep Exploitation

Charlie Miller and Chris Valasek, two security researchers, performed something incredible.

They hacked a Jeep while it was driving along a major highway at 70 mph, tampering with its entertainment system, engine, and brakes.

And they didn't do it in the rear seat; they did it from the comfort of a sofa in Miller's basement, 10 miles away.

6.6 How to Protect IoT Devices and Networks Against Cyber Hazards

1. Strong passwords

Before connecting to the network, devices connected to the Internet of Things should be secured. To do so, use strong passwords, keep these devices' security software up-to-date, and encrypt and authenticate the device.

2. Change Default Passwords

Many IoT devices come with default passwords, which cybercriminals are likely to know. It implies that you should change your default passwords to prevent unauthorized access to your Internet of Things devices.

3. Create guest networks.

It is critical to secure network connections and Wi-Fi with strong passwords. It is also necessary to create guest networks to prevent hackers from gaining access to the connection and ensure the security of your IoT devices.

4. Examine the default settings.

Many IoT devices include default privacy and security settings. To avoid uncertainty and cyberhazards, you should consider checking and changing them. Some default settings may be advantageous to the device manufacturer.

5. Maintain device updates.

Just like mobile updates, Internet of Things device manufacturers may send you updates to update and install new security software. You can also check their websites for updates and IoT protection.

6.7 How can IoT cybersecurity be improved?

In developing an IoT cybersecurity strategy, blockchain technology should be considered as a core approach. This is because blockchain is a decentralized storage space that houses information in a digital format that is accessible in a transparent manner. This is since blockchain has many entry points rather than a single point of contact. Because each node is essentially any electronic device that maintains a copy of the blockchain, an hazard on one or more of the nodes has no effect on the other nodes. By default, blockchain protects against data tampering by restricting access to IoT devices, allowing compromised devices in the network ecosystem to be shut down.

There are several steps that can be taken to improve IoT cybersecurity.

- When evaluating, selecting, and installing IoT devices, cybersecurity is a top priority from the start. Device security is not an afterthought and should never be added after the fact.
- Patches to cybersecurity software and firmware do reduce cyber risks. Consider investing only in IoT devices that can run the software and will accept software updates on a regular basis.
- Be proactive in terms of IoT device security. Freeware is rarely officially maintained in the cloud, at the edge, or on the device. The cost of attempting to recover from a cyberhazard is greatly outweighed by securing the IoT device and network in advance to prevent the hazard from occurring in the first place.
- Don't be afraid to seek professional assistance. Cybersecurity is an ever-changing target. Hackers always seem to be one step ahead of the competition. As a result, cybersecurity has become a skill that many organizations lack.

- Smart cybersecurity practices are difficult to envision and implement. They do, however, necessitate a continuous commitment to be fully effective. As a result, a proactive and systemic approach to cybersecurity will pay off in the short and long term.

6.8 IoT Security Issues and Solutions

1. Issue: Password security flaws

- Hard-coded and embedded credentials pose a risk to IT systems and are equally dangerous to IoT devices.
- Guessable or hard-coded credentials provide an opportunity for hackers to hazard the device directly.

- With default passwords, the hazarder may already know the machine's password!
- The Mirai malware is an example of a recent IoT hazard.
- Mirai infected IoT devices ranging from routers to video cameras and video recorders by successfully logging in with a list of 61 commonly used hard-coded default usernames and passwords.
- The malware spawned a massive botnet. It "enslaved" 400,000 interconnected devices.
- Mirai-infected devices (which became "zombies") were used to launch the world's first 1 Tbsp. distributed denial-of-service (DDoS) hazard on servers at the heart of internet services in September 2016.
- It brought Amazon Web Services and its clients, including GitHub, Netflix, Twitter, and Airbnb, to a halt.

Solution

Change the default password of your IoT device as soon as you receive it. Hackers use hash key decryption software with a database of common passwords and hash keys. It is

strongly advised to restrict logins to a single IP address. This severely restricts cross-border access.

2. Issue: Absence of consistent updates and fixes, as well as a faulty update mechanism

- IoT products are designed with usability and connectivity in mind.
- They may be secure at the time of purchase, but they become vulnerable when hackers discover new security flaws or bugs.
- IoT devices become vulnerable over time if they are not fixed with regular updates.
- Let us discuss this IoT security issue with Satori.
- Satori is malware that behaves and spreads similarly to Mirai.
- Satori transmits a worm, allowing infection to spread from device to device with no human intervention.
- First, it does not spread solely through credential guessing but has been discovered to target known vulnerabilities in specific Wi-Fi router ranges.
- Second, Satori has been found infecting smart processor architectures that had previously been ignored by IoT malware, SuperH, and ARC.

Solution

Any third-party software or hardware that is to be included in the supply chain should be thoroughly scanned by OT managers and other security experts. At all times, secure and encrypted channels should be used for frequent updates and secure update mechanisms. Before uploading updates to the IoT device network, their integrity and source should be verified. Enterprises can address IoT security issues by avoiding insecure device operating system customization.

3. Issue: Inadequate data security (communication and storage)

- Insecure communications and data storage are the most common causes of data security concerns in IoT applications.
- One of the major issues for IoT privacy and security is that compromised devices can be used to access sensitive data.
- Darktrace researchers revealed in 2017 that they had discovered a sophisticated hazard on an unnamed casino.

Solution

Cryptography is a powerful tool for dealing with data security issues.

To ensure confidentiality and privacy, businesses should use strong data encryption. This is useful during a data breach or a cyber-hazard.

It is critical to incorporate Federated Machine Learning (which is still in the development stage). In FML, the remains local while machine learning occurs at the edge. Only analytics are sent to the cloud. This can significantly reduce many IoT security challenges.

4. Issue: The Internet of Things Skill Gap

- Training and upskilling programs must be implemented.
- Additional informative workshops, hands-on newsletters, and bulletins, and "Hacker Fridays," where team members can attempt to hack a specific smart device, can make a significant difference.
- The more knowledgeable and prepared your team members are about IoT, the more powerful your IoT will be.

Solution

Adapting to changing needs puts a company under pressure on all fronts. Is your company prepared to adapt to such a shift? This is an issue that must be addressed and will necessitate a long-term strategy. How will you close the skill gap?

- **Retraining and upskilling:** With an abundance of resources, businesses can sponsor employee retraining and upskilling in emerging technologies. This should be viewed as an essential component of an enterprise's IT budget. According to reports, this approach improved employee retention and loyalty among IT behemoths.
- **Recruitment Strategy:** Rather than attempting to meet today's needs, businesses should focus on recruiting for an unknown tomorrow.
- **Building a future pipeline:** Tomorrow's needs, whether for the company or the customers, should be understood today. Developing a pipeline of cybersecurity professionals—those who can take on IoT security challenges and, most importantly, those who can bring organizational changes in IoT connectivity—should be pursued and integrated into the organization.

Chapter 6- Internet of things and security

6.9 Iot Security technologies

According to Forrester's research, the following are the most popular IoT security technologies.

1. Need for Security in IoT Networks

IoT network security is more difficult than traditional network security because communication protocols, IoT security standards, and device capabilities are more diverse, posing significant issues and increasing complexity. It entails securing the network connection that connects the IoT devices to the Internet's back-end systems.

2. IoT identification

It allows users to authenticate Internet of Things (IoT) devices, including managing multiple users for a single device and utilizing various authentication procedures, from several static passwords to more secure mechanisms like two-factor authentication, digital certificates, and biometrics. Many IoT authentication scenarios are M2M-based and do not include human involvement, in contrast to conventional enterprise networks where authentication is carried out by a human entering a credential. Baimos Technologies, Covisint,

Entrust Datacard, and Gemalto are some examples of vendors.

3. Encryption of IoT Devices

Protecting data integrity, avoiding data sniffing by hackers, and encrypting data while it is in transit and at rest between IoT edge devices and back-end systems. Standard encryption methods and protocols are inaccessible due to several IoT hardware profiles and devices.

4. Analytics for IoT Security

This technology collects, aggregates, monitors, and normalizes data from IoT devices and provides actionable reporting and alerting on suspicious activity or activity that violates established policies.

5. API Security for IoT

Using documented REST-based APIs, we can authenticate and authorize data movement between IoT devices, back-end systems, and applications. API security ensures the integrity of data transiting between edge devices and back-end systems, as well as the detection of potential menace and hazards against APIs. Akana, Apigee/Google, Axway, CA

Technologies, Mashery/TIBCO, MuleSoft, and others are examples of vendors.

Chapter 6- Internet of things and security

CHAPTER 7

BLOCKCHAIN SECURITY

Chapter 7 Blockchain security

7.1 Blockchain

Blockchain defined: Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk, and cutting costs for all involved.

7.2 Core Components of Blockchain Architecture:

- Node - user or computer within the blockchain architecture (each has an independent copy of the whole blockchain ledger)
- Transaction - smallest building block of a blockchain system (records, information, etc.) that serves as the purpose of blockchain.
- Block - a data structure used for keeping a set of transactions which is distributed to all nodes in the network.
- Chain - a sequence of blocks in a specific order

- Miners - specific nodes which perform the block verification process before adding anything to the blockchain structure.
- Consensus (consensus protocol) - a set of rules and arrangements to carry out blockchain operations.

7.3 Blockchain Importance

Business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

7.4 Key elements of a blockchain

Distributed ledger technology

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the

duplication of effort that's typical of traditional business networks.

Immutable records

No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

Smart contracts

To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.

7.5 How does blockchain work?

As each transaction occurs, it is recorded as a "block" of data.

Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what,

when, where, how much and even the condition — such as the temperature of a food shipment.

Each block is connected to the ones before and after it.

These blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together to prevent any block from being altered or a block being inserted between two existing blocks.

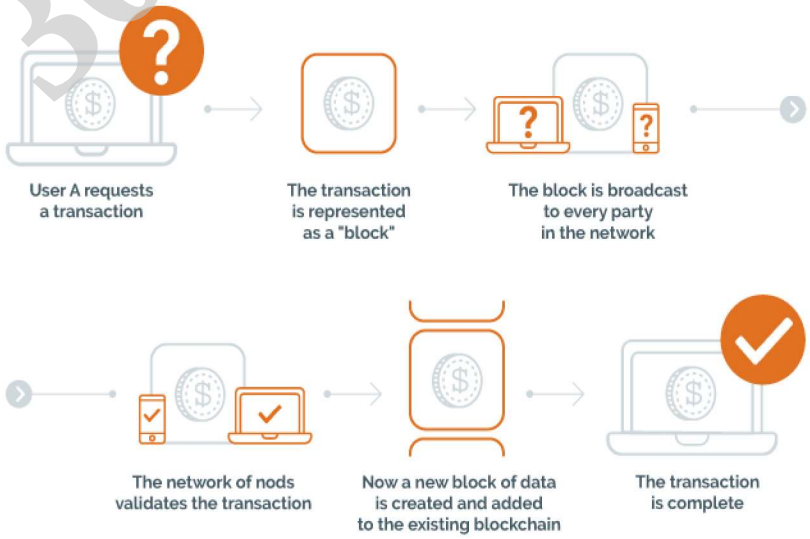
Transactions are blocked together in an irreversible chain: a blockchain.

Each additional block strengthens the verification of the previous block and hence the entire blockchain. This renders the blockchain tamper-evident, delivering the key strength of immutability. This removes the possibility of tampering by a malicious actor — and builds a ledger of transactions you and other network members can trust.

the past few years, Blockchain security has taken the world by storm. Its ability to create a secure and tamper-proof network for transactions has made it an incredibly valuable tool. Blockchain technology was first developed in 2008 for

the cryptocurrency Bitcoin. However, the potential applications of Blockchain extend far beyond cryptocurrencies. Today, blockchains are being used for everything from supply chain management to identity verification.

Blockchain technology is revolutionizing the world as we know it. But with great power comes great responsibility- and this is especially true when it comes to Blockchain security. In this post you will know about Blockchain security, from the basics to more advanced concepts. We will also provide tips on how to stay safe while using Blockchain technology. Also, you can consider taking an online Blockchain technology course to pump up your Blockchain security knowledge and skills.



Chapter 7 – Blockchain Security

7.6 Basic Blockchain Security

When it comes to security, Blockchain technology is often lauded for its tamper-proof and distributed ledger features. However, it's important to remember that no system is completely secure. To ensure the safety of your data, it's crucial to understand the basics of Blockchain security.

One of the key advantages of Blockchain is that it allows decentralized control. There is no central authority that can be hacked or taken offline. Instead, the network is made up of nodes, each of which stores a copy of the Blockchain. In order for a hacker to tamper with the Blockchain, they would need to hack every single node in the network - an extremely difficult feat.

Another important security feature of Blockchain is its cryptographic hashing. This allows each block in the chain to be uniquely identified and linked to the previous block. As a result, it's nearly impossible to insert bogus data into the Blockchain without raising suspicion. Any attempt to do so would require not only changing the data in the block, but also all subsequent blocks - an impractical task for even the most skilled hacker.

While Blockchain technology is certainly impressive from a security standpoint, it is important to remember that no system is impenetrable and there are some Blockchain security vulnerabilities as well. Thus, to protect your data, it is important to take basic security precautions as discussed further.

How is Blockchain Used for Security?

A Blockchain is a shared database that is managed by a network of computers rather than a single party. This decentralized structure allows for increased transparency and security, as each party on the chain can verify every transaction against the entire history of the Blockchain.

The key to understanding how Blockchain works is to think of it as a digital ledger. In traditional ledgers, transactions are recorded and managed by a central authority, such as a bank or government. In contrast, blockchains are decentralized, meaning that there is no central authority managing the ledger. Instead, the ledger is shared among all parties on the chain.

Each time a new transaction occurs, it is recorded on the Blockchain. These transactions are then verified by all parties on the chain using complex mathematical algorithms.

Once a transaction is verified, it cannot be changed or deleted. This creates a permanent and secure record of all transactions that have ever occurred on the Blockchain.

The decentralized nature of blockchains makes them particularly well-suited for applications that require increased transparency and security, such as financial transactions or supply chain management.

Thus, blockchains are still one of the most promising new technologies to emerge in recent years. This is why there is a high jump in applicants looking for Blockchain security jobs and projects. With their ability to provide increased security and transparency, they have the potential to revolutionize many industries and change the way we interact with technology in our everyday lives.

7.7 Blockchain Types and Security Menace

There are 4 types of Blockchain namely:

1. Public Blockchain

Public blockchains, such as Bitcoin, are open to anyone. Anyone can view the transaction history and create new transactions. Public blockchains are decentralized and secure, but they can be slow and expensive. Because public

blockchains are open and accessible to anyone, they are often more secure than private or permissioned blockchains. This is because it is much more difficult for bad actors to achieve a 51% hazard on a public Blockchain than it is on a private blockchain.

2. Private Blockchain

It is a distributed database that allows only approved members to have access to the data and perform transactions. Private Blockchains are usually permissioned, meaning that there is a central authority that controls who has access to the network. This contrasts with public Blockchains, such as Bitcoin, which anyone can join.

Private Blockchains are often used by businesses or other organizations where security and privacy are paramount. Since only approved members have access to the data, it is more difficult for hackers to breach the network. In addition, transactions on a private Blockchain can be carried out faster than on a public Blockchain since there is no need to wait for consensus from all members of the network.

Private Blockchains are sometimes considered less secure, as they rely on a single entity to maintain security. This

means that if the entity is compromised, the entire network can be disrupted.

3. Hybrid Blockchain

It is a type of Blockchain that combines the features of both public and private blockchains. A hybrid Blockchain can be customized, where users can decide who can take part within the Blockchain or which transactions are made public. A hybrid Blockchain has the benefits of both public and private blockchains.

The security drawback is that maintaining a real-time record of all users' preferences becomes very difficult for the central authority. This is why many reputable websites offer Blockchain security certification for free to help users enlighten about various security issues and give them basic related skills.

4. Consortium Blockchain

Consortium blockchains include known participants preapproved to participate in the consensus by a central authority within a Blockchain network. A consortium Blockchain allows only pre-selected nodes to participate in the consensus process. Consortium blockchains are often

used in business settings where there is a need for increased security and speed, but where decentralization is not a priority.

For example, a group of banks may use a consortium Blockchain to streamline their back-end operations. By pre-selecting who can participate in the network, they can be sure that only trusted actors are able to access sensitive data. This can help to improve efficiency while still maintaining security. Coming to security, they are less secure than public blockchains and more secure than private ones.

How Fraudsters Hazard Blockchain Technology?

Blockchain and data security are always a topic of concern for users. Blockchain technology also deals with security vulnerabilities, and it is vulnerable to **four types of hazards**: phishing, routing, Sybil, and 51% of hazards.

1. Routing Hazard

Another type of hazard that can occur in Blockchain technology is a routing hazard. This is when hackers intercept data as it's transferring to internet service providers. By doing this, they can disrupt the network and prevent transactions from being completed.

Routing hazards can be difficult to detect and prevent, but there are some measures that can be taken. For example, data can be encrypted before it's sent, and node operators can monitor their networks for suspicious activity. If possible, try to hire the best crypto auditors to be on the safe side.

2. Sybil Hazard

A Sybil hazard is a type of Blockchain hazard where hackers create and use many false identities to crowd the network and crash the system. This can be done by creating multiple accounts, computers, or ids. Sybil hazards can reduce confidence in the Blockchain, as well as lead to financial losses. To prevent a Sybil hazard, it is important to have strong security measures in place. This may include using digital signatures or ids, as well as maintaining a list of known ids.

3.The 51% Hazard

A 51% hazard is a type of Blockchain hazard where a group of miners or a single miner controls more than 50% of the network's mining power. This control allows them to manipulate the ledger, which could lead to double-spending or other types of fraud. While 51% hazards are very rare, they are a serious security concern for Blockchain security.

To protect against them, it is important for Blockchain networks to have a large and decentralized mining community.

These are just a few of the many ways that can impact Blockchain cybersecurity and cause harm.

Blockchain Security for the Enterprise

As enterprises increasingly explore the use of Blockchain technology, security concerns must be addressed to ensure that data is protected. There are several security controls that should be considered when implementing a Blockchain solution for an enterprise.

1. Identity and access management (IAM) is important to ensure that only authorized users have access to the system.

2. Key management is also critical, as private keys are needed to sign transactions and unlock data.

3. Data privacy must be considered to protect sensitive information from being accessed by unauthorized individuals.

4. Secure communication must be established between nodes to prevent eavesdropping or man-in-the-middle hazards.

5. Smart contract auditing is also essential to prevent vulnerabilities that could be exploited by hazarders. An authentic smart contract auditing service helps enterprises launch and maintain their Blockchain applications.

6. Finally, transaction endorsement can help increase a Blockchain's security by requiring multiple parties to sign off on each transaction.

Blockchain Penetration Examination

Blockchain technology is gaining traction in various industries, from banking and finance to healthcare and supply chain management. Interested learners can even opt for Blockchain Solution Architect training to understand the basics of blockchain architecture and design an application.

As the use of Blockchain grows, so does the need for effective penetration examination services. Blockchain penetration examination helps assess Blockchain applications' security and identify vulnerabilities that hazarders could exploit.

Functional examination, performance examination, API examination, security examination, and integrating examination are all essential components of effective Blockchain penetration examination. During a penetration examination, ethical hackers attempt to identify and exploit vulnerabilities in the system. This helps to find and fix potential exploits before criminals can use them.

What are Blockchain Security examination Tools?

There are several Blockchain Security examination tools available on the market today. Here is a brief overview of some of the more popular options:

1. **Truffle** –Truffle is a popular Ethereum development framework with a suite of tools for examination and debugging smart contracts.

2. **Ganache** – Ganache is a personal Ethereum Blockchain that can be used for examination and development. It includes a user interface for interacting with smart contracts.

3. **Examination** – Examination is a Node.js-based simulator for Ethereum smart contracts. It allows you to examination contracts on a simulated Ethereum network.

These are just some of the most popular Blockchain Security examination tools. There are many others available, each with its unique features and capabilities. Choosing the right tool for your needs will depend on the specific requirements of your project.

7.8 Blockchain Security Tips and Best Practices

There are certain Blockchain security tips and practices that apply to everyone:

1. Implementing Two-factor Authentication

One of the most important aspects of security in the Blockchain space is two-factor authentication (2FA). Implementing 2FA adds an extra layer of security to your online accounts by requiring a second factor, in addition to your password, to log in. This second factor can be a one-time code generated by an authenticator app, a hardware token, or a biometric factor like your fingerprint or iris scan.

While 2FA is not foolproof, it significantly increases the security of your online accounts and should be used whenever possible. In the Blockchain space, 2FA is especially important due to the high value of digital assets and the often-irreparable damage that a hack or theft can

cause. Also, try to find reputable Blockchain security audit companies that can identify any loopholes in the system and eliminate any vulnerabilities.

2. Allow Listing Trusted Senders and Recipients

One of the best things you can do to secure your Blockchain platform is to allow only trusted senders and receivers. This may seem like a no-brainer, but it's incredibly important. By allowing only trusted entities to interact with the Blockchain, you can dramatically reduce the chances of malicious activity. Of course, this doesn't mean you should never allow new entities onto the Blockchain.

Rather, it simply means that you should be very careful about who you allow access to. Take the time to verify the identity of each sender and receiver identity, and ensure they are credible before allowing them onto the network.

3. Keep your Software Up to Date

That means installing security updates and patching any vulnerabilities as soon as they are discovered. By staying on top of the examination security menace, you can help ensure that your Blockchain network remains safe and secure. Additionally, it's important to choose a reputable and reliable

provider for your Blockchain security needs. Look for a provider with a proven track record of keeping their networks safe and secure.

4. Using VPNs - Virtual Private Network

While the use of VPNs is not new, it is gaining popularity due to increased awareness of online security menace. A VPN is a secure, encrypted connection between two devices. This connection can tunnel data traffic through an untrusted network like the internet.

By encrypting the data traffic, a VPN can help to protect your information from malicious actors. In addition, a VPN can also help to improve your privacy by hiding your real IP address and location. While there are many different VPN providers to choose from, selecting a reputable provider with strong encryption and security features is important.

5. Use Anti-Phishing Tools

Phishing hazards are becoming increasingly common and can be difficult to detect and prevent. An anti-phishing tool can help to identify and block phishing attempts, keeping your Blockchain safe. Additionally, it's important to be aware of the signs of a phishing hazard. Be suspicious of any

email or message that asks you to click on a link or provide personal information. If you are skeptical about the legitimacy of an email, contact the sender to verify its authenticity.

CHAPTER 8

BIG DATA SECURITY

Chapter 8 Big Data security

8.1 Big data Definition

Big data is a combination of structured, semi-structured, and unstructured data collected by organizations that can be mined for information and used in machine learning projects, predictive modelling, and other advanced analytics applications.

Systems that process and store big data have become a common component of data management architectures in organizations, combined with tools that support big data analytics.

Big data characteristics

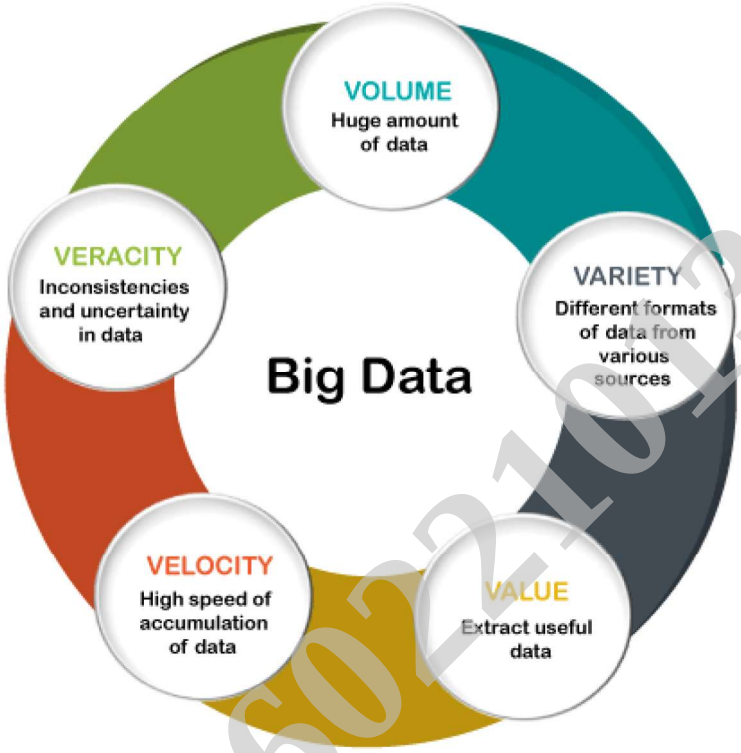
Big data is a collection of data from many different sources and is often described by five characteristics: volume, value, variety, velocity, and veracity.

- **Volume:** the size and amount of big data that companies manage and analyze
- **Value:** the most important "V" from the perspective of the business, the value of big data usually comes from insight discovery and pattern recognition that led to more effective operations, stronger customer relationships, and other clear and quantifiable business benefits.

- **Variety:** the diversity and range of different data types, including unstructured data, semi-structured data, and raw data
- **Velocity:** the speed at which companies receive, store, and manage data, e.g., the specific number of social media posts or search queries received within a day, hour, or other unit of time.
- **Veracity:** the "truth" or accuracy of data and information assets, which often determines executive-level confidence

The additional characteristic of variability can also be considered:

- **Variability:** the changing nature of the data companies seek to capture, manage, and analyze—e.g., in sentiment or text analytics, changes in the meaning of key words or phrases



8.2 Big data security

Big data security is the process of monitoring and protecting a company's important business data with the goal of ensuring a safe and compliant ongoing operation.

Big data security is a constant concern because big data deployments are valuable targets for would-be intruders. A single ransomware hazard might leave a company's big data deployment subject to ransom demands. Even worse, an unauthorized user may gain access to a company's big data to siphon off and sell valuable information. The losses can be severe. A company's IP may be spread everywhere to

unauthorized buyers, and it may suffer fines and judgements from regulators.

Securing big data platforms takes a mix of traditional security tools, newly developed toolsets, and intelligent processes for monitoring security throughout the life of the platform.

8.2.1 How Big Data Security Works?

Big data security's mission is clear enough: keep out unauthorized users and intrusions with firewalls, strong user authentication, end-user training, and intrusion protection systems (IPS) and intrusion detection systems (IDS). In case someone does gain access, encrypt your data in transit and at rest.

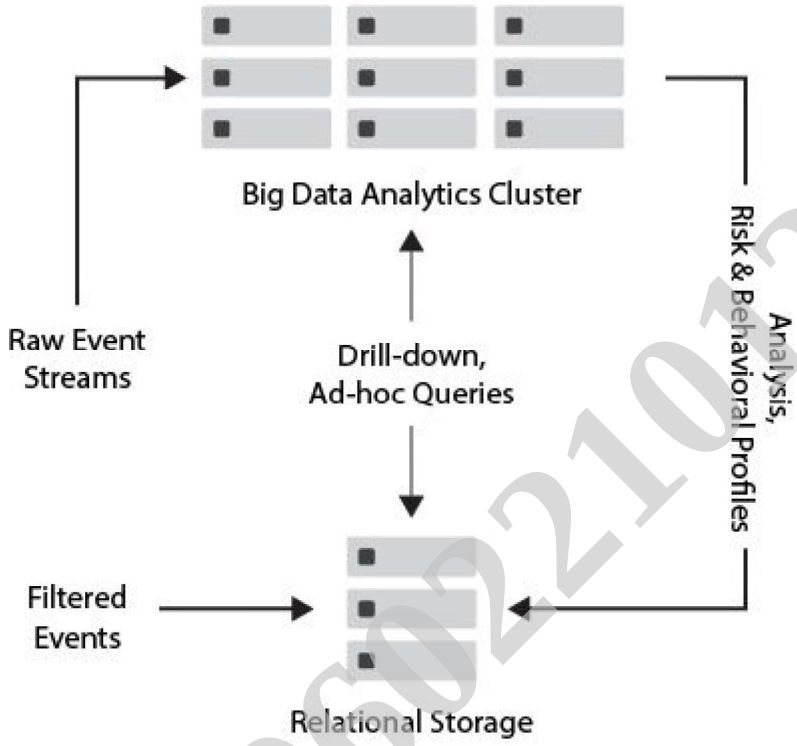
This sounds like any network security strategy. However, big data environments add another level of security because security tools must operate during three data stages that are not all present in the network. These are: data ingress, which is what's coming in; stored data; and data output going out to applications and reports.

Stage 1: Data Sources Big data sources come from a variety of sources and data types. User-generated data alone can include CRM or ERM data, transactional and database data, and vast amounts of unstructured data such as email

messages or social media posts. In addition to this, you have the whole world of machine-generated data, including logs and sensors. You need to secure this data in transit, from sources to the platform.

Stage 2: Stored Data Protecting stored data requires mature security toolsets, including encryption at rest, strong user authentication, and intrusion protection and planning. A company needs to run its security toolsets across a distributed cluster platform with many servers and nodes. In addition, its security tools must protect log files and analytics tools as they operate inside the platform.

Stage 3: Output Data The entire reason for the complexity and expense of the big data platform is so it can run meaningful analytics across massive data volumes and different types of data. These analytics output results to applications, reports, and dashboards. This extremely valuable intelligence makes for a rich target for intrusion, and it is critical to encrypt output as well as ingress. Also, secure compliance at this stage: make certain that results going out to end-users do not contain regulated data.



Big Data security is routed through a circuitous path, and in theory could be vulnerable at more than one point.

8.3 Benefits of Big data Security

A big data security solution may assist businesses everywhere by enhancing client retention, risk identification, business innovation, cost control, and efficiency.

Some major advantages of big data security include:

- **Customer Retention:** With big data security, a company can observe many data patterns, which allows them to better fit their products and services with their client's needs.

- **Risk Identification:** Because of big data security, a company can use big data tools to identify risks in their infrastructure, helping them create a risk management solution.
- **Business Innovation:** Big data security can help companies update their tools and transfer products to new secure systems. This innovation can improve business processes, marketing techniques, customer service, and company productivity.
- **Cost Optimization:** Big data security technologies can reduce customer costs by efficiently storing, processing, and analyzing large volumes of data. Big data security tools will also calculate how the product will benefit the company, so companies can pick a company that is better for their infrastructure.

8.4 Challenges of big data security

There are several obstacles to big data security that could potentially compromise it. Remember that these difficulties are not at all exclusive to on-premises big data platforms. They also apply to clouds. Take nothing for granted while hosting your big data platform in the cloud. Strong security service level agreements can help you and your provider

meet these similar issues.

The main obstacles to big data security are listed below:

- **Newer technologies can be vulnerable.** Advanced analytic tools for unstructured big data and nonrelational databases (NoSQL) are examples of newer big data technologies in active development. It can be difficult for security software and processes to protect these new toolsets.
- **Variable impact:** mature security tools effectively protect data ingress and storage. However, they may not have the same impact on data output from multiple analytics tools at multiple locations.
- **Access without permission:** big data administrators may decide to mine data without permission or notification. Whether the motivation is curiosity or criminal profit, your security tools need to monitor and alert you to suspicious access, no matter where it comes from.
- **Beyond routine audits:** The sheer size of a big data installation, terabytes to petabytes large, is too big for routine security audits. And because most big data platforms are cluster-based, this introduces multiple vulnerabilities across multiple nodes and servers.

- **Requires constant updates:** If the big data owner does not regularly update security for the environment, they are at risk of data loss and exposure.

8.5 Big data security technologies

All these big data security solutions, including user access control and encryption, are not new. Their scalability and capability to protect several types of data at various stages are novel features.

- **Encryption:** To protect data across enormous data volumes, your encryption techniques must be able to safeguard it both in transit and at rest. Additionally, encryption must function on a wide range of data types, including both user- and machine-generated data. Additionally, encryption tools must function with various analytics toolkits and the data produced by them, as well as on popular big data storage formats, including relational database management systems (RDBMS), non-relational databases like NoSQL, and specialized filesystems like Hadoop Distributed File System (HDFS).
- **Centralized Key Management:** Centralized key management is a security best practice that has been around for a while. Big data settings, particularly ones

with broad global dispersion, can benefit from it just as much. On-demand key distribution, logging, policy-driven automation, and separating key administration from key usage are all examples of best practices.

- **User Access Control:** Although user access control is perhaps the most fundamental network security measure, few businesses use it because of how expensive it can be to operate. This can be terrible for the big data platform and is already risky at the network level. A policy-based strategy that automates access based on user and role-based parameters is necessary for strong user access management. Complex user control levels, such as numerous administrator settings that defend the big data platform from insider assaults, are managed by policy-driven automation.
- **Intrusion Detection and Prevention:** Systems for intrusion detection and prevention are the workhorses of the security industry. They remain just as useful to the big data platform despite this. The importance of big data and its distributed design encourage infiltration attempts. Security administrators may defend the big data platform from hazard using IPS,

and should an intrusion succeed, IDS quarantines it to prevent more serious damage.

- **Physical security:** Keep in mind the importance of physical security. Build it into the deployment of your big data platform in your own data center, or carefully do research on the data center security of your cloud provider. Strangers or employees who shouldn't be in critical areas might be denied entry to data centers by physical security measures. The same will be true for security logs and video surveillance.

8.6 Implementing Big data security.

Here are some suggestions for implementing big data security, whether you're just getting started with big data management and seeking initial big data security solutions or you are an experienced big data user and require updated protection:

- **Effectively manage and educate internal users:** As previously said, unintentional security blunders made by staff members present one of the most often exploited security vulnerabilities for bad actors. Provide only the bare minimum of data source access to each user depending on their function, set mobile and corporate device regulations, and train your staff on security and credential management best practices.

- **Plan frequent security monitoring and audits**: It's critical to routinely evaluate how the network and dat a landscape has changed over time, particularly in lar ger organizations where big data and software are growing almost daily. There are several network monitoring technologies a nd third- party services available on the market, allowing your security personnel immediate access to users and strange behavior. Regular security audits also give your team the chance to evaluate larger scale concerns before they develop into actual security risks.
- **Deal with a trusted big data company:** Most companies that offer big data storage, analytics, and managed services do so with some level of security included, or they collaborate with one. Talk to your providers about your security concerns, legal needs, and big data use cases so they may tailor their services to what you need. The platform you choose may not have all the exact capabilities that your business or particular use cases require.

8.7 Big data security Companies

Snowflake

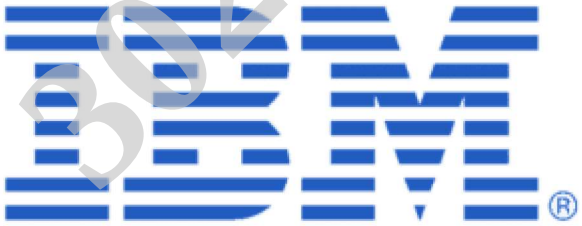
Snowflake's team of data experts believes that data security should be natively built into all data management systems rather than added on as an afterthought. Snowflake's Data Cloud includes comprehensive data security features like data masking and end-to-end encryption for data in transit and at rest. They also offer accessible support to their users, allowing them to submit reports that Snowflake and their partner, Hacker One, can analyze while running their private bug program.

Teradata

Teradata is a top provider of database and analytics software, but it's also a major proponent and provider of cloud data security solutions. Their managed service, called Cloud Data Security As-a-Service, offers regular third-party audits to prepare for data regulatory committee audits. They also offer features such as data encryption in transit and at rest, database user role management, storage device decommissioning, cloud security monitoring, and a two-tiered cloud security defense plan.

IBM

IBM's data security portfolio focuses on multiple environments, global data regulations, and simple solutions so that users can easily manage their data sources and security updates after deployment. Some of the main areas that IBM pays attention to for data security include hybrid cloud security management, embedded policy and regulation management, and secure open-source analytics management.



CHAPTER 9

Discussion Questions about security and examination

Chapter 9: Discussion Questions about security and examination

It has become quite essential for organizations to find and assess vulnerabilities in their system. The system's security has become a big deal in modern application development. Business logic has become more complicated than ever, and many web applications are incorporating new things. In such a scenario, incorporating security examination has become quite important.

9.1 Security Examination

Security examinations are a procedure where examination is done to find any weaknesses in the security mechanism that protects the data and keeps functionality as intended. The main components of security are authentication, authorization, availability, confidentiality, integrity, and non-repudiation.

Important information related to security examination:

- In security scanning the need for vulnerability scanning helps in identifying the loopholes in the system. The use of vulnerability management software helps to identify and omit those security risks.
- Security examination also deals with resolving misconfigurations in the software, network, and

systems. Both manual and automated tools are available for in-depth analysis and fixing the issue.

- There is an additional security measure known as penetration examination that helps in stimulating a real-time cyber-hazard on the software. It helps to detect the system capability to handle bot hazards.
- Ethical hacking is also a part of security examinations. It helps in saving all the misconfigurations and vulnerabilities in software.

1. What is "System Weakness"?

Any system that is weak enough to be hazarded by outsiders or bugs is said to be vulnerable.

The likelihood of vulnerabilities increases if the system has not undergone rigorous security examination. Patches or fixes are needed periodically to shield a system from vulnerabilities.

2. How does security examination work?

The method of security examination involves running examination cases to find flaws in the information systems' security mechanisms. Examiners play the part of hazarders and manipulate the system to uncover flaws in the security procedures. The purpose of security

examinations to identify any application or system's vulnerability and secure its data from intruders.

3. How does loop examination operate, and what is it?

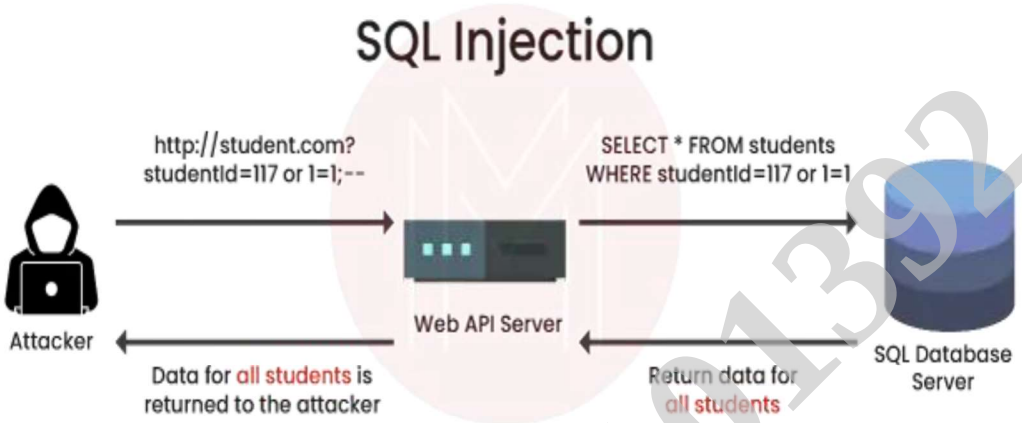
Software examination, known as "Loop Examination", focuses solely on ensuring that loop structures are correct. It belongs to the Control Structure Examination (path examination, validation examination of data, condition examination).

Loop examination is white box examination. The loops in the program are examinations using this technique.

4. Define SQL injection.

When using code injection to target data-driven systems, SQL injection inserts malicious SQL statements into the entry field for execution. It is primarily identified as a website hazard vector, although it may also be used to hazard any kind of SQL database. Hazarders can become administrators of the database server, spoof identities, alter already-existing data, cause repudiation problems like cancelling transactions or changing balances, allow full disclosure of all data on the system, destroy data, or otherwise make it unavailable, and cause repudiation issues.

Chapter 9- Discussion Questions about security and testing



5. Define Adhoc Examination?

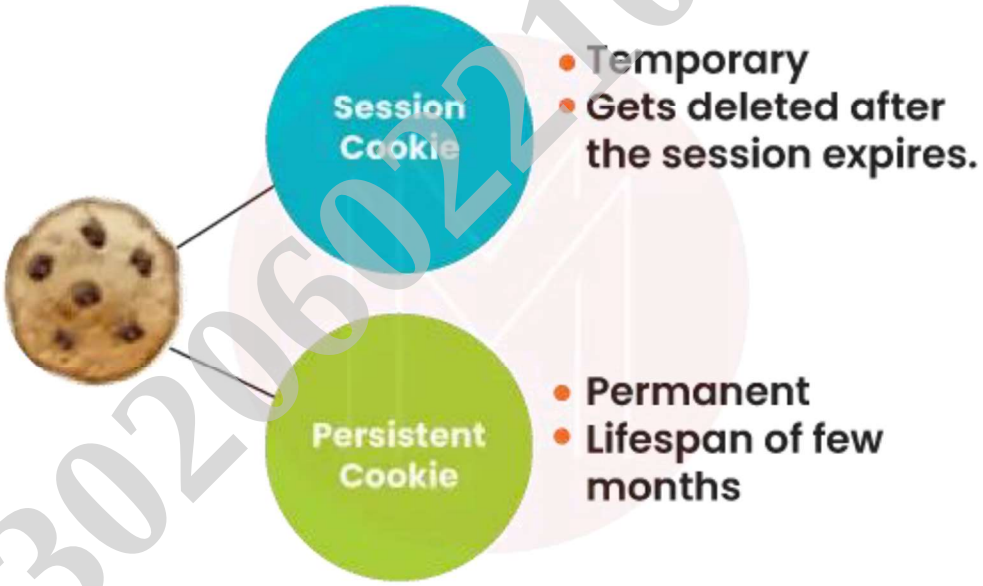
Adhoc examination is commonly used to break the system intentionally. The most notable feature of Adhoc examination is the absence of any examination design methodology for producing examination cases. The method is typically applied to find software bugs. Adhoc examinations are frequently performed without documentation because it lacks examination cases.

6. What are cookies, and what varieties are there?

A cookie is a little piece of data that a web browser stores after receiving it from a web server and can access at any time in the future. Cookies include password-based data, auto-fill data, etc.

Session cookies and persistent cookies are the two sorts of cookies.

Session cookies are transient and only exist for the duration of the current session. Persistent cookies are the ones that are kept on a hard drive and remain there until they expire or are manually deleted.



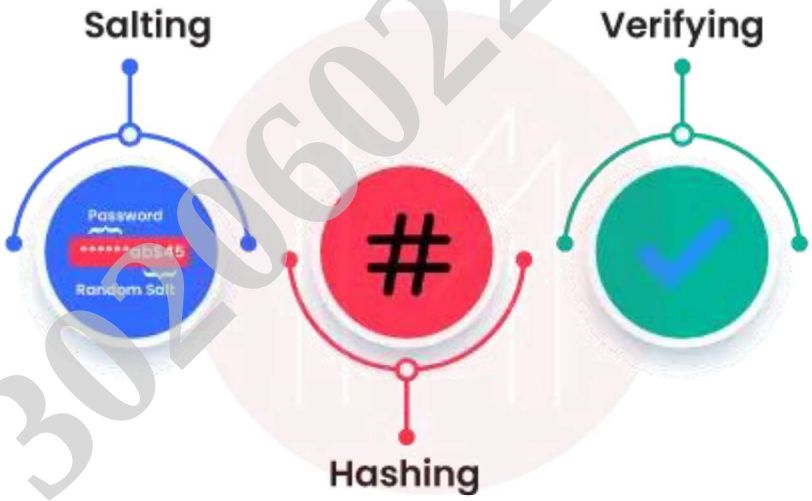
7. What's the prime difference between Structured Examination and Unstructured Examination?

Structured Examination: In this approach, each step of the examination process, from the creation of examination cases to the subsequent sequential execution, is documented. The examiners do

examinations according to this script. Unstructured examination: In this method, examination cases are created as they go along by the examiners, who often do examination by guessing incorrectly.

8. What are the two popular methods for safeguarding a password file?

Hashed passwords and salt values, or password file access control, are two popular methods for securing a password file.



9. Define the system examination in software examination.

The entire system must be examinationed as part of system examination. To determine whether the system operates according to plan, all the modules and components are connected. System examination is done

after integration examination. For the creation of high-quality products, this is essential.

10. Describe ISO 17799.

Best practices for Information Security Management are outlined in ISO/IEC 17799, which was first published in the UK. It contains information security rules for all enterprises, no matter how big or little.

11.Name the three security examination techniques.

Security examination approaches include white-box examination, black-box examination, and grey-box examination.

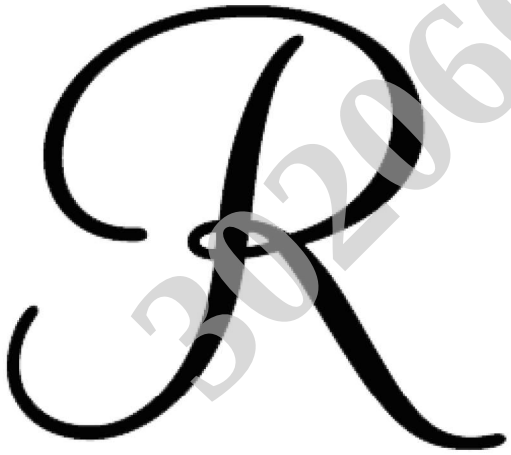
- **White Box Examination:** Under this type of examination, all the data is made available to the examiners.
- **Black Box Examination:** Using this technique, the system can be examination in a real-time setting without the examiners providing any information.
- **Grey Box Examination:** White box examination and black box examination are combined in one technique, known as grey box examination. The examiners receives only a portion of the information; the rest is examination independently.

12. List the seven primary security examination categories according to the Open-Source Security examination methodology guide.

According to the Open-Source Security examination methodology document, there are seven primary categories of security examination:

- **Weakness Points Scanning:** Automated software checks a system for known flaws.
- **Security Scanning:** Network and system vulnerabilities can be found using security scanning, a manual or automated process.
- **Penetration examination:** Security examination that helps to identify flaws in a system is known as penetration examination.
- **Security Auditing:** A thorough examination of systems and applications to find flaws.

- **Ethical hacking:** Hacking for purposes other than obtaining personal gain is known as ethical hacking.
- **Posture Assessment:** An organization's total security posture is shown by a posture assessment, which incorporates security scanning, ethical hacking, and risk assessments.



REFERENCES

References

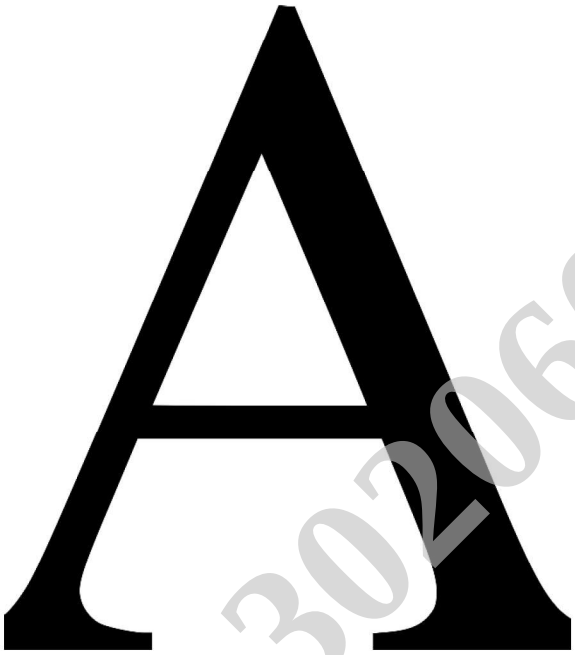
References

- Stamp, M. (2011). *Information security: principles and practice*. John Wiley & Sons.
- Bertino, E., & Sandhu, R. (2005). Database security-concepts, approaches, and challenges. *IEEE Transactions on Dependable and secure computing*, *2*(1), 2-19.
- E. Bertino and R. Sandhu, "Database security - concepts, approaches, and challenges," in IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 1, pp. 2-19, Jan.-March 2005, doi: 10.1109/TDSC.2005.9.
- Using Artificial Intelligence in Cybersecurity. (2023). Retrieved from balbix: https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/
- D., L. (2023, September 1). What Is Web Application Security, How It Works, and Best Security Practices for 2023. Retrieved from Hostinger Tutorials: https://www.hostinger.com/tutorials/web-applicationsecurity?ppc_campaign=google_search_generic_hosting_all&bidkw=defaultkeyword&lo=9112360&gclid=Cj0KCQjwib2mBhDWARIsAPZUn_kVBdu2xB_hKXyHXUAL3iM2ku2z_NNntinqzSJPOwRlcFGF_eUUVTYaArQ7EALw_wcB
- Crocket, E. (2023). What is Big Data Security? Challenges & Solutions. Retrieved from Datamation: https://www.datamation.com/big-data/big-data-security/

- Sajd, H. (2023). AI in Cybersecurity: 5 Crucial Applications. Retrieved from V7: https://www.v7labs.com/blog/ai-in-cybersecurity

- Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering*, *59*, 183-187.
- Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

References



Assignments

Assignments

Assignment Chapter 1 (Introduction to Data Security)

Part 1 Choose the correct answer.

1- A set of guidelines, policies, and procedures that organizations use to manage their data

a. Data Governance

b. Data management

c. Data Integration

d. Data security

2- A ……. must guarantee that the information inside that domain is correctly maintained across various platforms and business processes.

a. Data owner

b. Data user

c. Data custodian

d. Data Stewards

3- …… oversees managing the quality of the defined datasets daily. They are called the Subject Matter Expert (SME).

a. Data owner

b. Data user

c. Data custodian

d. Data Stewards

Assignments

4- A …… is responsible for developing and maintaining security safeguards for specific data collection to fulfill the Data Governance Framework

a. Data owner

b. Data user

c. Data custodian

d. Data Stewards

5- The process of ensuring that the data is accurate, complete, and consistent. This includes processes for data validation, data cleansing, and data matching, as well as data quality metrics and data quality reporting.

a. Data integration

b. Data retention

c. Data quality

d. Data architecture

6- the process of storing data for a certain period, as per legal, regulatory and/or business requirements. It includes data archiving, data purging and data retention policies.

a. Data integration

b. Data retention

c. Data quality

d. Data architecture

Assignments

7- the process of analyzing data to extract insights and make better decisions. This includes data warehousing, data mining, and data visualization.

a. Data analytics

b. Data retention

c. Data quality

d. Data architecture

8- This component is often associated with secrecy and the use of encryption.

a. integrity

b. confidentiality

c. availability

d. privacy

9- The certainty that the data is not tampered with or degraded during or after submission. It is a certainty that the data has not been subject to unauthorized modification, either intentional or unintentional.

a. integrity

b. confidentiality

c. availability

d. privacy

10-

This implies that authorised users will have access to the in formation when it is required.

Assignments

a. integrity

b. confidentiality

c. availability

d. privacy

Part -2 Answer the Following Questions

1- discuss the main types of security hazards.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

2- Compare between Hackers and Crackers

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Assignments

Part3 – true or false

1- cryptography means covered writing
2- By creating backup copies of data, organizations can recover data should it be erased or corrupted accidentally or stolen during a data breach.
3- Text, audio, images, and videos all of these are forms of cryptography
4- the first 12 digits of a credit card number may be hidden within a database; this is an example for "Data Masking".
5- Crackers are people who hack a system by breaking into it and violating it with some bad intentions.
6- Data erasure is the process of gaining access to a computer or a network that might not be legal or permitted for any random user.
7- Masquerading is an hazard that could affect data integrity
8- Denial of service hazard is an hazard that could affect data availability
9- the replay hazard considered as a kind of the passive hazards
10- release of message content is an hazard that could affect data integrity

---

Assignment chapter 2 (Ethical Hacking)

1-Compare the different types of hackers.

……
……
……
……
……
……
……
……
……

Assignments

.....
.....
.....
.....
.....

2- What are the main characteristics of the ethical hacking process

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Assignment chapter 3 (Database Security)

1- Authentication and Authorization are considered types of

a- menace protection

b- access management

c-network management

d- Information protection

2- Auditing and menace detection are considered types of

a- menace protection

b- access management

c-network management

d- Information protection

3- It is a type of hazard which occurs when a malicious code is injected into frontend (web) apps and then transmitted to the backend database.

a- malware

b- SQL injection

c-Ransomware

d- DOS hazard

Assignments

4- …….. is software designed to corrupt data or harm a database. It could enter your system via any endpoint device connected to the database's network and exploit vulnerabilities in your system.

a- malware

b- SQL injection

c-Ransomware

d- DOS hazard

5- An hazard in which the cybercriminal uses a huge number of fake requests to overwhelm the target service, the database server.

a- malware

b- SQL injection

c-Ransomware

d- DOS hazard

6- Discuss the different Control Measures for securing Data in Databases

Assignments

……
……
……
……
……
……
……
……
……

Assignment chapter 4 (web application)

(A. Session hijacking, B. Cross-site scripting (XSS), C.Sensitive data disclosure, D. Credential stuffing, E.SQL Injection, F. Security misconfiguration)

Choose the correct answer.

1.This is also known as data leakage or data exfiltration and can happen through a variety of channels, including email, cloud storage, social media, or through a data breach (……..)

2. This hazard involves taking over an active user session to gain unauthorized access to a web-based application. Techniques included are IP spoofing, side jacking, man-in-the-middle, and session fixation (……)

3. This hazard involves injecting malicious code into a web page that gets executed by the browser of the person visiting the page (……..……)

Assignments

4. This hazard involves using a list of stolen credentials (usernames and passwords) to attempt to gain unauthorized access to various online accounts (…….)
5. This type of flaw enables an hazarder to tamper with an application's database queries by injecting code (……)
6. This hazard exploits configuration vulnerabilities in a web application. (……)

Assignment chapter 5 (Artificial Intelligence security)

Answer The Following.

1- A technology that uses statistical techniques to give computer systems the ability to "learn" (e.g., progressively improve performance) using data rather than being explicitly programmed.

a- expert system

b- machine learning

c-Neural Networks

d- deep learning

2- ……...are programs designed to solve problems in specialized domains.

a- expert system

b- machine learning

c-Neural Networks

d- deep learning

3- AI in cybersecurity include applications such as

a- Malware and phishing detection

b- early menace detection

c- breach risk prediction

d- all the above

4- **AI-based cybersecurity systems can't detect malicious traits more effectively**.

a- true

b-false

5- **Phishing refers to the hacker sending malicious links to users (usually via email) to acquire sensitive information or disrupt the system. The malware is activated when the user clicks on the malicious link.**

a- true

b-false

6- Artificial intelligence can also analyze malware based on its inherent characteristics.

a- true

b-false

7- A manual menace detection and mitigation process gives an hazarder ample time to encrypt or steal data.

a- true

b-false

Assignments

8- Hackers can use AI techniques to develop intelligent malware that can modify itself to avoid detection by even the most advanced cybersecurity software.

a- true

b-false

9- AI systems, unlike any other software product, are not susceptible to cyberhazards. Hackers can't feed models poisonous data to alter their behavior according to their desired malicious intent.

a- true

b-false

10- Data manipulation, data unavailability, and intelligent malware are examples of the menace that could affect the Artificial Intelligence systems

a- true

b-false

Assignment chapter 6 (Internet of things and security)

1-A network of interrelated devices that connect and exchange data with other devices and the cloud.

a- big data

b- Internet of things

c- artificial intelligence

d- blockchain

Assignments

2- **IoT security management includes _____**

a- Data storage

b-Protocol abstraction

c-Simple and fast installation

d-Security with hardware

3- Discuss the elements that could be affected if there're any IOT hazards occur?

……

……

……

……

……

……

……

……

……

……

……

……

4- **How to Protect IoT Devices and Networks Against Cyber Hazards?**

Assignments

……

……

……

……

……

……

……

……

……

……

5- Cryptography is a powerful tool for dealing with data security issues.

a- true

b-false

6- IoT network security is the same as the traditional network security

a- true

b-false

7- Standard encryption methods and protocols are inaccessible due to several IoT hardware profiles and devices.

a- true

b-false

Assignments

Assignment chapter 7 (Blockchain Security)

1. Is Blockchain totally secure?

.....
.....
.....
.....
.....
.....
.....
.....

2. How is Blockchain used for security?

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

3. What are the problems with Blockchain security?

.....
.....
.....
.....
.....
.....
.....

Assignments

.....
.....
.....
.....
.....
.....
.....

Assignment chapter 8 (Big data Security)

1- Define the Big data and how to secure it?

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Assignments

2- what are the benefits and challenges of securing big data?

……

……

……

……

……

……

……

……

……

……

……

Assignments

Lecturer's Biography

Ass.Prof. Shimaa M. Ouf is currently an associate professor and the head of the Information Systems Department, Faculty of Commerce and Business Administration, Helwan University, Cairo, Egypt. She was born in Cairo, Egypt. She received the M.Sc. degree in information systems from the Faculty of Computers and Information, Helwan University, Egypt, and held a Ph.D. degree in information systems from the Faculty of Computers and Information, Helwan University, Egypt.

DR. Soha Ahmed is currently a lecturer in the Information Systems Department, Faculty of Commerce and Business Administration, Helwan University, Cairo, Egypt. She graduated from the business information system department, faculty of commerce and business administration, Helwan University. She received her master's degree in information technology from the Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt. And she was granted her Ph.D. in business information systems, faculty of commerce and business administrations at Helwan University.

Biography