Building an Impenetrable Vault: Advanced Cybersecurity Strategies for Database Servers

Md Shariar Sozol[1], Md Minhazul Islam[2], Md Mostafizur Rahman[3], Md Arafath Uzzaman[4], Md Zamshed[5], Golam Mostafa Saki[6]

[1] Master of Cybersecurity (Extension) & University of Technology Sydney (UTS), Australia
[2] Master of Information Technology (Extension) & University of Technology Sydney (UTS), Australia
[3] Master of Engineering (Extension) & University of Technology Sydney (UTS), Australia
[4] Master's Programme in Electrical Engineering & Lappeenranta–Lahti University of Technology (LUT), Finland
[5] MSc in Engineering Management University of South Wales, United Kingdom (UK)
[6] MSc in Engineering Management & University of South Wales, United Kingdom (UK)

---***---

Abstract - Organizations are relying more on database servers as storage for important information. This makes it imperative for strong measures against cyber-attack to safeguard sensitive data. The study focusses on some advanced ways of protecting database servers from cyber-crime and these are: SQL injection prevention, role-based access control, data encryption techniques, and insider threat mitigation. It also looks into the latest developments in the area such as machine learning based abnormality detection, Zero Trust architecture, and multi-factor authentication. Such practices make it possible to establish a multi-layered defensive mechanism that enhances data protection by considering the outside as well as inside dangers. Besides compliance with regulations, maintaining visibility and patch management is vital so as to remain ahead of changing cyberspace dangers. Therefore, this research presents an array of recommendations to address the entire security landscape for resilient database platforms against sophisticated assaults. The conclusions point out that there is need to amalgamate these practices towards ensuring safety in terms of risks related with contemporary database server setups.

Key Words: Database Security, SQL Injection, Role-Based Access Control, Data Encryption, Insider Threat, Zero Trust Architecture.

1.INTRODUCTION

All existing data-driven operations are largely supported by database servers in today's digital economy. Financial institutions, healthcare providers, e-commerce platforms and government agencies among other users depend heavily on these servers for storage, management and protection of their sensitive information. Nevertheless, with the increased volume and sensitivity of data comes an escalation of possible cyber-attacks against them. They are no longer secure repositories for online sensitive files because threat actors from hacking groups with incredibly advanced skills to rogue employees have all turned to them as soft targets to steal, alter or erase information from databases. Unfortunately, such breaches wreak havoc leading to financial losses; loss of esteem; penalties imposed by authorities; even disruptions in operations.

Organizations are now focusing on securing their database servers in order to protect the data assets they have from hackers. Nevertheless, the changing nature of cyber threats has rendered traditional methods of preventing them insufficient. A wide range of tactics such as SQL injection, brute force attacks, privilege escalation and insider threats among others have been used by attackers to evade defenses and gain unauthorized entry. In response to this, database server cyber security strategies have moved towards a multi layered approach that utilizes advanced technologies and best practices with a focus on increasing the strength of systems against outside and inside dangers.

Code flaws typically surface in software scripts, like for instance, the prominent SQL injection vulnerability [1]. Thus, the source code review and analysis is the foundation of the task of finding the weaknesses. Big data technologies can be chosen depending on factors that satisfy the necessities of a company.

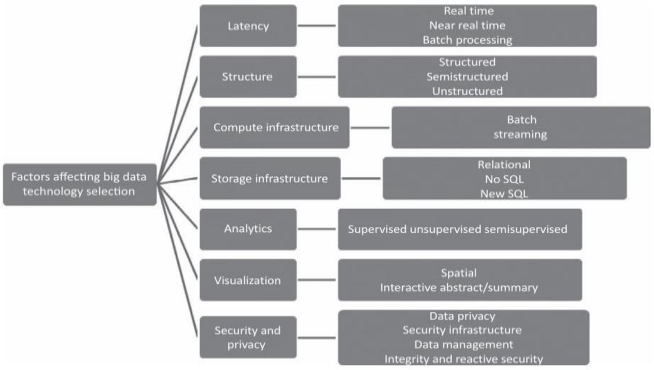
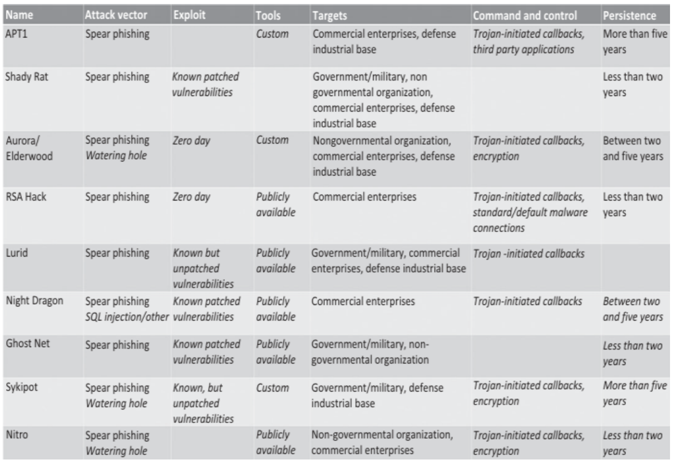


Figure 1.1: Factors affecting Big Data Analytics [2].

These elements encompass the period of delay in response time, the level of organizing in which data exists, specification of an SQL environment required, kinds of anticipated analytics, particular kinds of visual illustrations that may be required and finally societal demands for safety as well as your organizational requirements. Various big data technologies might be selected according to these aspects [2].

This research paper investigates essential practices that organizations ought to adopt in order to create a virtual impenetrable box around their database servers (Comprehensive Database Security). The core principles, being both elementary and more complex ones such as multi-factor authentication (MFA), role-based access control (RBAC), transparent data encryption (TDE) and zero trust architecture among other things will be explored. In their application over time these methods enable robust security frameworks which are capable of reducing various forms of attack vectors. In addition, emerging solutions like machine learning driven anomaly detection as well as intrusion detection systems (IDS) are discussed in the paper since they improve real time monitoring while enhancing threat recognition capabilities.



Name	Attack vector	Exploit	Tools	Targets	Command and control	Persistence
APT1	Spear phishing		*Custom*	Commercial enterprises, defense industrial base	*Trojan-initiated callbacks, third party applications*	More than five years
Shady Rat	Spear phishing	*Known patched vulnerabilities*		Government/military, non governmental organization, commercial enterprises, defense industrial base		Less than two years
Aurora/ Elderwood	Spear phishing *Watering hole*	*Zero day*	*Custom*	Nongovernmental organization, commercial enterprises, defense industrial base	*Trojan-initiated callbacks, encryption*	Between two and five years
RSA Hack	Spear phishing	*Zero day*	*Publicly available*	Commercial enterprises	*Trojan-initiated callbacks, standard/default malware connections*	Less than two years
Lurid	Spear phishing	*Known but unpatched vulnerabilities*	*Publicly available*	Government/military, commercial enterprises, defense industrial base	*Trojan -initiated callbacks*	
Night Dragon	Spear phishing *SQL injection/other*	*Known patched vulnerabilities*	*Publicly available*	Commercial enterprises	*Trojan-initiated callbacks*	*Between two and five years*
Ghost Net	Spear phishing	*Known patched vulnerabilities*	*Publicly available*	Government/military, non-governmental organization		*Less than two years*
Sykipot	Spear phishing *Watering hole*	*Known, but unpatched vulnerabilities*	*Custom*	Government/military, defense industrial base	*Trojan-initiated callbacks, encryption*	*More than five years*
Nitro	Spear phishing *Watering hole*		*Publicly available*	Non-governmental organization, commercial enterprises	*Trojan-initiated callbacks, encryption*	*Less than two years*

Figure 1.2: APT Characteristics [3].

This research also emphasizes the necessity of governance, compliance, and regular patch management beyond technical controls. Data protection is enforced by law, such as in GDPR, HIPAA and PCI DSS which need stringent controls on data protection; following these regulations is relevant for legal compliance and effective safety from cyber threats. Routine audits, patching and updates address vulnerabilities leading to their prompt solution reducing the chances of exploits.

The aim of this research project is to develop a holistic guide for securing database servers against the most common and dangerous threats to cyber security. The organizations can create a lasting database environment through the use of multiple defenses at various levels combined with proactive monitoring and adaptable security policies that not only resist attacks but also guarantee indisputable protection for their most precious information.

2. Threats to Database Servers

In the present digital environment, database servers encounter a variety of risks, which can be generally divided into outside assaults, dangers from within and conditions that make them vulnerable. It is important to understand them so as to put proper counter actions in place. In this paper, we will describe the ways of threats to database servers –

1. Physical Threats to Database Servers and
2. Cyber Threats to Database Servers

We will put much priority and focus on cyber threats and mitigation rather than physical one for this research paper.

2.1. Physical Threats to Database Servers

Unauthorized Access to Server Room: As far as physical threats go, one of the most commonly experienced is unauthorized access to server rooms. Attackers are capable of accessing database servers' rooms and thereby modifying equipment, taking storage devices away from them or even making copies of confidential information if they can go in there freely. Some of the effective ways to prevent unauthorized access include biometric authentication systems, security badges and surveillance systems.

Theft of Storage Devices: Theft of hard drives or SSDs as well as backup tapes can lead to data security concerns. Attackers will easily retrieve any sensitive information contained inside these devices if they are not encrypted after gaining physical possession over them. This risk can be reduced through encryption for data at rest along with storing storage devices inside locked tamper-proof cabinets.

Tampering with Hardware: Hardware tampering can be done by would-be attackers who insert malicious components like keyloggers or hardware backdoors into server hardware. Therefore, sensitive data will be captured or remote access to the server granted. Regular monitoring, tamper-evident seals, and trustworthiness of the hardware parts might assist in preventing tampering.

Destruction of Infrastructure: When servers are deliberately destroyed as a result of vandalism or target attacks, this can result in catastrophic data loss and downtime. If there are no proper safeguards like fire suppression systems or disaster recovery plans then anything from fire, water damage or physical impacts would lead to irreversible loss of information which is very costly [4].

Environmental Attacks: environmental factors such as extreme temperature, humidity or fluctuation in power can compromise database servers. In some cases, attackers would purposely adjust controls within their environment so as to make server overheating possible or electrical surges that can destroy consistency hardware components. One way to defend against such an action is by establishing strict monitoring systems specifically designed for server rooms.

Social Engineering: Not just limited to phishing, social engineering can entail impersonating authorized personnel physically to access server rooms. Attackers impersonating IT staff, maintenance workers or even delivery personnel can bypass physical security controls. Due to this, it is important that the employees be trained in how to identify suspicious activities and report them.

Interference with Power Supply: The attackers can cause power supply disruption to server rooms leading to abrupt shutdowns and data corruption. UPSs and backup generators play a major role in avoiding loss of data as a result of power interruptions. Furthermore, ensuring that power cables and line supplies are secure from tampering is crucial.

2.2. Cyber Threats to Database Servers

There are diverse cyber threats that database servers confront, each of them exploiting different weakness points. Organizations must deal with the following critical threats:

SQL Injection: SQL injection is a pervasive assault during which hackers derive database access or manipulate databases by inserting disallowed SQL queries into input areas. The susceptibility of this kind of attack could be attributed to weak user input validation and improper application of parameterized queries. Data theft, unauthorized access or total database hijack can all be results on successfully carried out SQL injections.

Privilege Escalation: Another form of threat that organizations face is privilege escalation that occurs when attackers take advantage of flaws in software vulnerabilities or access controls to obtain elevated rights. These people would have the opportunity to view secure data, alter system settings and set up pathways for their future attacks. This risk is more serious since it puts an intruder in charge of vital database infrastructures.

Brute Force and Dictionary Attack: Brute force and dictionary attacks are typically performed using automated programs that try to guess user passwords by entering many different combinations in quick succession and these types of attacks occur against weakly protected accounts or those that have poorly set up authentication mechanisms. Hackers can corrupt database integrity and availability once they gain access.

DDoS Attack: DDoS attack involves flooding a database server making it impossible for lawful customers to get in. Such attacks may also serve as camouflage when other malicious processes such as extracting data take place unnoticed. DDoS incidents may come with prolonged periods during which there's no service leading to disruptions of business activities and great losses in money.

Man-in-the-Middle Attack (MitM): A MitM attack is when attackers intercept communication between a database server and users, usually by using unsecured or poorly configured network connections. Eavesdropping on or changing data in transit can be done by attackers who want to steal credentials, sensitive information, or manipulate transactions. MitM attacks show how important it is to use SSL/TLS for encrypting data during transmission [5].

Denial of Services (DoS) Attack: A DoS attack usually comes from one source unlike DDoS attacks which have multiple sources. The goal is the same: to flood the database server with traffic or resource-hungry requests that cause it to crash or become unavailable. These attacks can be particularly effective against smaller-scale database systems with limited capacity Quantum attack environments are much easier for attackers to break into fiber optic cables than bombarding a server with requests, as is done during a traditional denial of service attack (DoS). In this instance the open optical quantum transmitting devices would be completely blocked so that light cannot pass through. The purpose of a quantum denial of service attack is just to interrupt any process without any need for acquiring the phone number [5].

Insider Threats: An employee, contractor, or any other trusted person misuses his legitimate access to attack the database in insider threats. Insider threats are either intentional or accidental but pose significant risks in both cases. A malicious insider could steal information while an unintentional one might leak some confidential details due to negligence. Detecting insider threats is challenging and requires advanced monitoring systems as well as strict access controls.

Trojan Horse Attack: In the case of QKDs, a Trojan horse attack is known as a gigantic pulse attack. Notably, though, quantum and classical Trojan horses differ in their modes of operation. For instance, laser beams would be launched into some quantum channel before their returns are studied as opposed to employing some malware package which is simply too remote from reality. The slightest number of reflected photons could enable an eavesdropper to determine one of the basic choices made by the lawful participants [5].

3. Typical Practices for Database Servers Cybersecurity

These best practices function as integral parts of an all-encompassing database security plan:

Authentication and Access Control: Database security heavily relies on solid authentication and access control systems. For instance, only those authorized can perform certain activities or get specific types of information through multi-factor authentication (MFA) and adherence to the principle of least privilege. Indeed, this proves consistent with individuals' characters and inclinations in their use of systems. A classic scenario concerns the creation and storage of passwords that pose certain risks to these systems. For instance, it is dangerous when passwords are identical across several platforms, thereby creating a single point of vulnerability. Also, saving passwords within the system or on paper may seem easier but can pose significant threats to security given that it is in a not completely safe area [6]. Likewise, mechanisms like two-factor authentication must be examined attentively regarding potential users who will utilize them. In addition, role-based access control (RBAC) is a system that allows for easier handling of access permissions as it assigns them according to individuals' places in an organization rather than everyone else.

Encryption Strategies: Data encryption serves as a basic way of securing sensitive information. Transparent Data Encryption (TDE) provides security for data which is not in use by encrypting at the level of storage without any human intervention either from an administrator or software developer end [5]. For the data being moved, SSL/TLS protocols are employed to ensure that data circulation is safeguarded against interception. Therefore, efficient key management techniques play an important role in keeping encryption effective and avoiding wrong logins to access keys. Standard confidentiality access controls have been mostly created for internal services and certainly depend heavily on the system for authentication. Therefore, one simple way out is for the user to encrypt every document before putting it in the cloud. But that also means he/she won't be able to search through them. The next option would then be to either provide the encryption key to the cloud provider or download everything back into a local machine and decrypt it there. Hence, these alternatives lack privacy as well as efficiency [7].

Regular Patching and Updating: Maintenance of security patches just in time is crucial for fighting against disclosed vulnerabilities. Database software updates can be ensured with the automated patch management systems resulting in lower risk of exploits. Leaving patches unattended may expose the systems to certain exploits that could have otherwise been prevented. One such instance is the simple matching coefficient (SMC). Considering two applications that are not affected by the vulnerability patch, when studying its impact on software. This is some useful information that we need to capture. Hence, in this situation symmetric coefficient would be used [8].

Network Segmentation: The database servers are separated from one another through network segmentation which diminishes the chances of sideways migration once an intrusion takes place. There are several cyber security threats including fraud, malware incursions and network attacks that can be detected using graph-based anomaly detection methods. However, there are as yet some areas that need more of our attention. For instance, one possibility is to utilize the graph algorithms for pre-filtering alerts from firewall and other cyber security systems. Such an imposition would greatly reduce the workload on security analysts while enhancing the overall security posture [9].

Firewall Configuration: Firewalls can filter out any superfluous traffic and allow only essential access for the ongoing process. In order to reduce possible areas to target during attacks, rules applied by firewalls and also access control lists (ACLs) on networks can be used to minimize threats. An example of a method is being able to use graphs as algorithms that help remove alerts that come from firewall systems or other cybersecurity systems in advance. One option, for example, is to pre-filter alarms from firewalls and other cybersecurity systems using graph-based algorithms [9]. This will significantly lessen the burden on security analysts while at the same time raising the general level of security. Through this research paper, an overview has been given on existing procedures for identifying anomalies in cyber security through graphs [9].

Database Activity Monitoring and Auditing: Database activities can be detected suspiciously earlier through continuous monitoring. Logging and auditing techniques provide an audit opinion which can be analyzed during or after an occurrence. Regular audits assist organizations in discovering vulnerabilities and observing adherence to regulatory frameworks. For instance, cluster headers with comparable properties that were received in unusually high quantities on a single server in a network traffic database stood out as a collective anomaly [9].

4. Advanced Cybersecurity Measures for Database Servers

Intrusion Detection and Prevention System (IDPS): When IDPS are built up at the network and database levels, they can assist in intrusion detection and response. As well as using behavioral analysis, these systems can detect threats using signature-based detection. As is common with other enterprises, this institution has a network-based Intrusion Detection

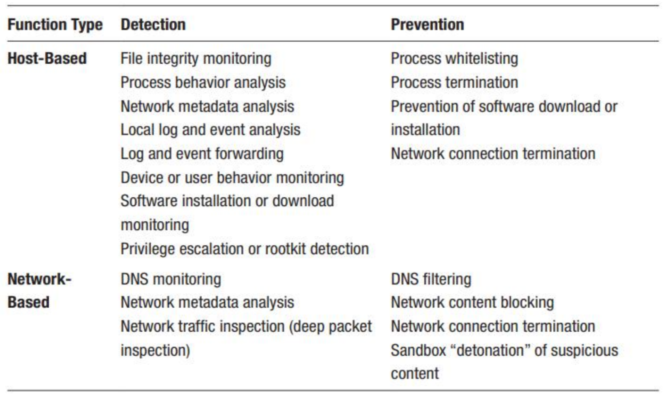
System/Intrusion Prevention System (IDS/IPS) in place. They have a combination of modules running within their Next-Generation Firewalls (NGFWs) as well as some deployment of an open-source IDS/IPS. These systems are used for sensing anomalies and responding to them using both automated and manual responses by their Security Operations Center [10].

However, over time their IDS has been less effective due mainly to growth in size and complexity of the network, adoption of cloud-based resources where it cannot be an inline "chokepoint" and increased use of encrypted protocols. They want a more elaborate and comprehensive method for detecting and responding to indicators of compromise across their heterogeneous environment. To them it appears that they are wasting too much time and money while achieving only limited results. Ideally, they would like to have one place for defining IDS policies, plus different places in order to enforce them across the entire organization including user devices and workloads within the company [10]. Additionally, they desire quantitative benefits such as reduced noise or false positives along with qualitative benefits like improved case studies for security analyst decision-making contexts.

Such organizations likewise operate network-based intrusion detection systems/intrusion prevention systems (IDS/IPSs). This specific organization has designed its IDS using a hybrid approach with modules integrated into next generation firewalls (NGFW) as part of open-source tools. These systems are employed for monitoring abnormal activities on computers connected to those networks through automatically done actions from security departments which are used when needed to respond manually if necessary.

With regard to commercial IDPS, there exist two quite distinct methods that greatly vary in terms of deployment goals and locations, these are host-based and network-based [10]. It should also be noted that in most cases the prevention systems should have at least some ability to perform detection functions; in order for them to act on an undesirable (or at least unexpected) event, they must first identify such events.

1. Host Based and
2. Networked Based



Function Type	Detection	Prevention
Host-Based	File integrity monitoring Process behavior analysis Network metadata analysis Local log and event analysis Log and event forwarding Device or user behavior monitoring Software installation or download monitoring Privilege escalation or rootkit detection	Process whitelisting Process termination Prevention of software download or installation Network connection termination
Network-Based	DNS monitoring Network metadata analysis Network traffic inspection (deep packet inspection)	DNS filtering Network content blocking Network connection termination Sandbox “detonation” of suspicious content

Figure: Typical Intrusion Detection and Prevention Functions, by Deployment Model [10].

Network Traffic Analysis and Encryption: Modern application protocols utilize encryption (primarily TLS), for it ensures message integrity and confidentiality from network peers and intermediaries. As a result, even authorized network intermediaries performing security functions cannot see what is inside encrypted traffic.4 The way out they have is an established practice of making the intermediary an active participant in the conversation, terminating one encrypted link and initiating another to carry out traffic inspection.4 This is usually done via distributing an enterprise PKI-created certificate based upon a root of trust shared by both ends of the encrypted TLS connection, effectively amounting to a legitimate Man-In-The-Middle (MITM) attack [5].

Nonetheless, it is possible that this model is irrelevant for Zero Trust environments. Numerous Zero Trust implementations use mutual TLS (mTLS, also known as two-way TLS) for communications between the user agent PEP and the network PEP. In doing so, both PEPs validate one another’s certificate which improves security because an attacker cannot use a single stolen certificate to mount a man-in-the-middle (MITM) attack–he/she would require possession of both components’ certificates, a much less likely scenario. Some Zero Trust systems take this further by utilizing short-lived certificates for these communicators. As a result of this enhanced protection, conventional network Intrusion Detection and Prevention Systems (IDPS) located “in-between” PEPs cannot access encrypted sections of network traffic [10]. This means that even though the IDPS has access to the certificates that encrypt the application protocol, it cannot have access to the certificates that encrypt the Zero Trust tunnel.

Zero Trust and IDPS: Modern safety architecture needs IDPS - applied in its widest definition as a general series of functions throughout all platforms in an organization. This will remain relevant even as organizations transition to the Zero Trust security model. However, there is likely to be a shift in the way IDS/IPS operates after a Zero Trust approach has been implemented [10]. Organizations should know this and be ready to adapt. For instance, still on the zero-trust hypothesis; changes are likely within segmentation of networks and patterning of traffic encryption. In this case, firms might have to augment their host-based IDS/IPS or invest more towards making IDPS network-based which form part of Zero Trust system. About 80% of data breaches that target web applications, according to Verizon's data breach report for 2022, are caused by stolen passwords, which can happen as a result of brute force assaults or weak passwords [13]. For Zero Trust, the concept "Never Trust, Always Verify" is typical. The fundamental idea behind the Zero Trust security model is to shift the focus of defense from trusting users and devices on the network of the company to the users themselves. Additionally, the model consistently requests users' identities as they try to access more sensitive resources [13]. One popular IAM solution currently on the market is Okta, which may be used to implement Zero Trust. Continuous verification and least privilege access are the main points of Zero Trust models, which means authentication as well as authorization are required for each specific access request made by anyone anywhere. Okta is a cloud software that can function as an Identity Provider (IDP) or Service Provider (SP). It maintains the necessary user data in an Okta Universal Directory [13].

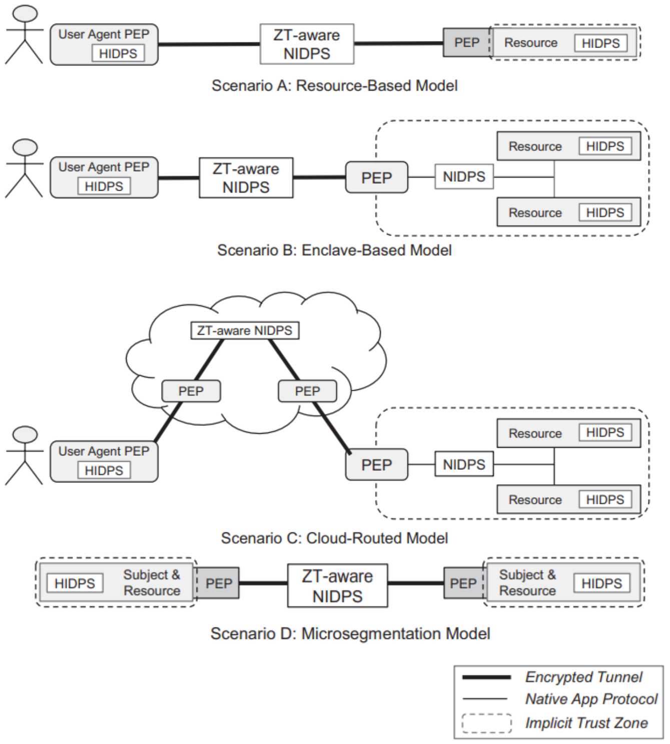


Figure: IDPS and Zero Trust Deployment Models [10].

Machine Learning for Threat Detection: By analyzing database traffic patterns that are not normal, machine learning models can enhance threat detection. Such models continue to learn over time and adapt to changes in order to defend against newly emerging threats.

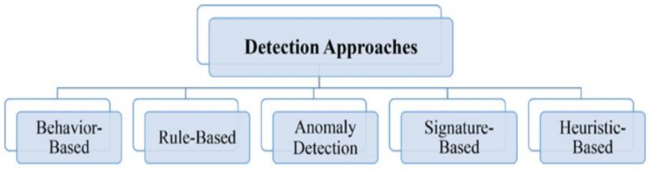


Figure: Threat Detection Approaches [11]

Traffic categorization as well as network intrusion detection and resource allocation rely greatly on machine learning (ML). Some scholars employed classic algorithms to achieve high accuracy in several issues while others applied hybrid methods.

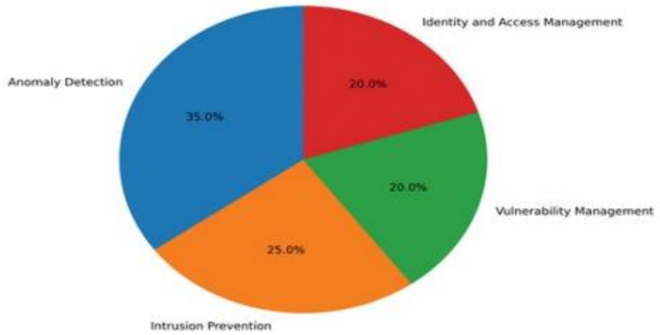


Figure: AI/ML usage in Security Automation [14].

In as much as each of these models has different phases that vary depending on the type of model being used, there are three main components of all these models; namely dataset, training and testing [12]. The methodologies for network security threats detection can be categorized into three classes according to model's working principle: Anomaly-based Detection; Stateful Protocol Analysis; Signature Based Detection among others. By using artificial intelligence's predictive powers to enhance threat detection and identification, threat hunting is transformed. Artificial Intelligence is able to identify significant patterns and filter out extraneous noise by efficiently processing and analyzing large amounts of data. An organization's network can analyze large amounts of endpoint data, and AI systems are capable of producing detailed application profiles that provide insights into typical operational patterns. By combining behavioral analysis with AI, a more dynamic approach to threat detection is made possible [14].

Data Masking and Tokenization: Masking and tokenization techniques can be used to protect sensitive data within non-production environments. Unlike the real data, these methods use imitations, but they also help with maintaining confidentiality when it comes to testing or development. One of the most crucial data preprocessing stages in the text classification task is tokenization, which also has a major impact on the model's performance [15].

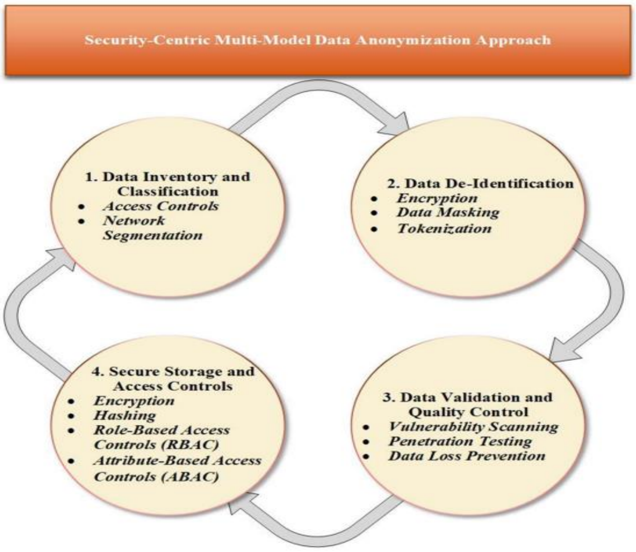

Security-Centric Multi-Model Data Anonymization Approach
1. Data Inventory and Classification
Access Controls
Network Segmentation
2. Data De-Identification
Encryption
Data Masking
Tokenization
3. Data Validation and Quality Control
Vulnerability Scanning
Penetration Testing
Data Loss Prevention
4. Secure Storage and Access Controls
Encryption
Hashing
Role-Based Access Controls (RBAC)
Attribute-Based Access Controls (ABAC)

Figure: Security-Centric Multi-Model Data Anonymization Approach [16].

Any Corporation uses data masking to further lower the danger of data re-identification. This implies that in order to hide the real data, sensitive data is substituted with false or random data. For instance, an employee's social security number could be masked by substituting a string of random letters and digits for the actual number rather than being stored [16]. To further lower the danger of reidentification, ABC Corporation also uses Tokenization techniques, which are similar to Data Masking. This entails substituting a distinct token or identifier for sensitive data. For instance, a token that can only be understood by authorized individuals could take the place of a credit card number [16].

Database Firewalls and Virtual Patching: Database firewalls are designed to filter and block unauthorized queries or commands that are not compliant with established security policies. When the official patches are absent, virtual patching can be used as a temporary measure for reducing risks arising from known vulnerabilities. While preserving the operational integrity of the database, an additional layer of protection is added.

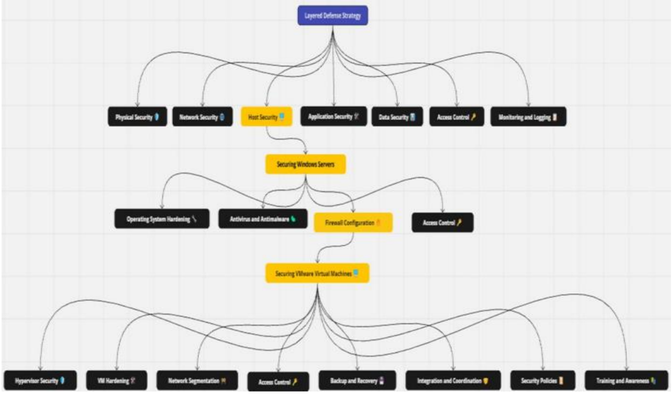


Figure: Layered Defense Strategy [17].

Hardening virtual machines and securing the hypervisor are just two components of a comprehensive strategy needed to secure VMware VMs. guaranteeing the safety of programs operating within virtual machines and servers. Update your virtual machines' operating systems frequently to guard against known vulnerabilities. To guarantee that virtual machines (VMs) are set in accordance with security best practices, create and use templates [17].

Securing Database Backup: With today's technology, people are creating vast amounts of data through the use of numerous apps, and this data is then stored in databases based on usage. Database technology offers secure, user-friendly, and effective methods for organizing and managing data and information. Database management systems (DBMS) and computer networks are used for all data modification and maintenance tasks [18]. DBMS has emerged as a potent tool for quick information interchange and access. Backup data is as prized as data in primary database servers. Securely encrypt the backup files before keeping them in separate secure locations. These backups should be regularly verified for their integrity and appropriate access controls kept against unauthorized entry. The backup procedure is not necessary to resolve IS issues. Critical information services remain available even in the event of a backup system failure. The backup process adds computational load, which is detrimental to the delivery of IS information services [19].

Vendor and Third-Party Management: Perform a thorough evaluation of a third-party vendor's security processes, including incident response protocols, data protection measures, and regulatory compliance, before working with them. Provide contractors with explicit and succinct contractual agreements that specify the security standards, data protection protocols, and breach reporting guidelines that they must follow [20]. To find and address such security weaknesses, make sure outside vendors go through routine security audits and assessments. To reduce the possibility of illegal access, restrict the access that third-party vendors have to critical systems and information. Use intrusion detection systems and monitoring tools to quickly identify and address any illegal access or questionable activity. Create a cybersecurity policy that describes the organization's goals for security, individual roles and duties, and incident response protocols. To defend against different kinds of cyber-attacks, use a combination of security measures, such as firewalls, antivirus software, and encryption [20].

5. Regulatory and Compliance Considerations

Database security is heavily reliant on adherence to industry regulations like GDPR, HIPAA and PCI DSS. Accordingly, many security measures and practices are enforced for organizations in order to keep sensitive information safe from hacks or legal repercussions. Companies continue to monitor existing legislation through regular compliance audits and evaluations. The General Data Protection Regulation, or GDPR for short, is a comprehensive data protection law that was put into effect in the EU on May 25, 2018 [21]. In the European Union (EU), the General Data Protection Regulation (GDPR) has brought about a new era of privacy rights for individuals by revolutionizing the handling and protection of personal data. GDPR ensures that companies and organizations handle personal data with the utmost care and responsibility thanks to its broad scope and strict guidelines.

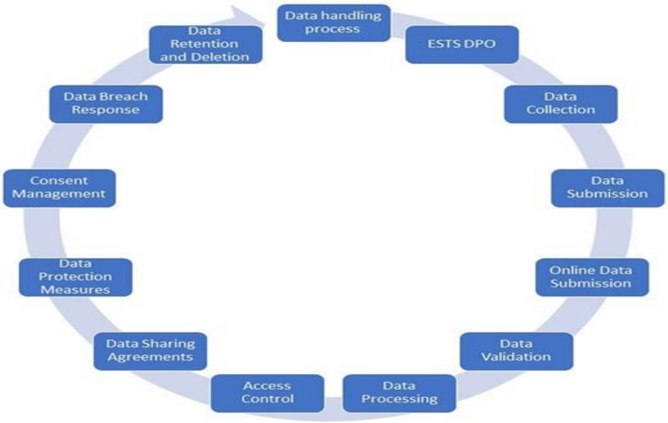


Figure: Processes within the ESTS database to adhere to GDPR [21].

The GDPR procedure carries a number of inherent risks. When information is accidentally or illegally exposed, especially health information, the right to human dignity may be breached. An individual's dignity may be gravely violated and compromised as a result of this unapproved revelation. Intentional or illegal linking of data inside a database might result in data processing that violates established principles and infringe the right to personal data protection. Transparency in data processing must be ensured, and this is mostly possible at the local level [21].

6. Future Trends in Database Security

Today's businesses face several obstacles due to the increased variety and complexity of data (unstructured/semi-structured), including indexing, sorting, searching, analyzing, and visualizing. The 5-v characteristics—Volume, Velocity, Veracity, Variety, and Value—are what consistently characterize big data. Nearly every big data model relies on these five-variable traits [22]. The need for database server security strategies to keep pace with changing cyber threats has increased. Database security will increasingly rely on new technologies such as quantum-resistant encryption, blockchain integration and AI-driven analytics. Furthermore, cloud-native database security solutions will grow in importance as more organizations embrace hybrid and multi-cloud deployments.

7. CONCLUSIONS

To protect a database server, it is important to use a comprehensive and multilayered approach that is aimed at addressing both traditional as well as new forms of threats around databases server security. Companies can build an unbreakable fortress for their database systems by installing strong authentication devices, using encryption methods, coming up with patch management processes and invest in advanced technology solutions. Moreover, safeguarding such data integrity and keeping its confidentiality up to date requires continuous inspection, periodical reviews while proactively embracing new practices with regard to security.

ACKNOWLEDGEMENT

We gratefully acknowledge to the International Journal of Scientific Research in Engineering and Management (IJSREM) for publishing our research paper on "Building an Impenetrable Vault: Advanced Cybersecurity Strategies for Database Servers."

REFERENCES

1. Yan, B., Cheng, Y., Shi, C., Fang, Y., Li, Q., Ye, Y., & Du, J. (2023). Graph Mining for Cybersecurity: A Survey. arXiv.Org. https://doi.org/10.48550/arxiv.2304.00485
2. Janeja, V. P. (2022). Big data analytics and its need for cybersecurity: Advanced DM and complex data types from cybersecurity perspective. In Data Analytics for Cybersecurity (pp. 60–77). Cambridge University Press. https://doi.org/10.1017/9781108231954.005
3. Janeja, V. P. (2022). Types of cyberattacks. In Data Analytics for Cybersecurity (pp. 78–90). Cambridge University Press. https://doi.org/10.1017/9781108231954.006
4. Elkhodr, M., Shahrestani, S., & Cheung, H. (2021). Database security and privacy for IoT applications: Best practices. Journal of Information Security and Applications, 58, 102734. https://doi.org/10.1016/j.jisa.2021.102734
5. M. S. Sozol, M. M. Rahman, M. M. Islam, and G. M. Saki, "Quantum Cryptography in Modern Cybersecurity," International Journal of Scientific Research in Engineering and Management (IJSREM), vol. 8, no. 8, pp. 1-12, Aug. 2024, doi: https://doi.org/10.55041/IJSREM37219
6. Janeja, V. P. (2022). Human-Centered Data Analytics for Cybersecurity. In Data Analytics for Cybersecurity (pp. 137–146). Cambridge University Press. https://doi.org/10.1017/9781108231954.011

7. Shahien, T., Sarhan, A. M., & Alshewimy, M. A. M. (2021). Multi-server searchable data crypt: searchable data encryption scheme for secure distributed cloud storage. Journal of Ambient Intelligence and Humanized Computing, 12(9), 8663-8681. https://doi.org/10.1007/s12652-020-02621-8
8. Janeja, V. P. (2022). Introduction to Data Mining: Clustering, Classification, and Association Rule Mining. In Data Analytics for Cybersecurity (pp. 29–59). chapter, Cambridge: Cambridge University Press. https://doi.org/10.1017/9781108231954.004
9. M. S. Sozol, G. M. Saki, and M. M. Rahman, "Anomaly Detection in Cybersecurity with Graph-Based Approaches," International Journal of Scientific Research in Engineering and Management (IJSREM), vol. 8, no. 8, pp. 1-7, Aug. 2024, doi: https://doi.org/10.55041/IJSREM37061
10. Garbis, J., & Chapman, J. W. (2021). Zero trust security : an enterprise guide. Apress. https://link-springer-com.ezproxy.lib.uts.edu.au/book/10.1007/978-1-4842-6702-8
11. Alzaabi, F. R., & Mehmood, A. (2024). A Review of Recent Advances, Challenges, and Opportunities in Malicious Insider Threat Detection Using Machine Learning Methods. IEEE Access, 12, 30907–30927. https://doi.org/10.1109/ACCESS.2024.3369906
12. Kalita, B., & Sarma, P. K. D. (2024). Network Security Threats Detection Methods Based on Machine Learning Techniques. In Advanced Computing, Machine Learning, Robotics and Internet Technologies (Vol. 1953, pp. 137–156). Springer. https://doi.org/10.1007/978-3-031-47224-4_13
13. Öberg A. What is Zero Trust: and How Can It Be Implemented? https://www.theseus.fi/bitstream/handle/10024/788457/Oberg_Andre.pdf?sequence=2
14. Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. DOI: https://www.doi.org/10.56726/IRJMETS32644
15. P. Prakrankamanant and E. Chuangsuwanich, "Tokenization-based data augmentation for text classification," 2022 19th International Joint Conference on Computer Science and Software Engineering (JCSSE), Bangkok, Thailand, 2022, pp. 1-6, https://ieeexplore.ieee.org/abstract/document/9836268
16. Şahin, Y., & Dogru, İ. (2023). An enterprise data privacy governance model: security-centric multi-model data anonymization. International Journal of Engineering Research and Development, 15(2), 574-583. https://dergipark.org.tr/en/download/article-file/3039865
17. Gudimetla, S. R., & Kotha, N. R. Layered Defenses: Securing Windows Servers and VMware Virtual Machines. https://www.researchgate.net/profile/Sandeep-Gudimetla/publication/383269590_Layered_Defenses_Securing_Windows_Servers_and_VMware_Virtual_Machines/links/66c58bfe4b25ef677f727e05/Layered-Defenses-Securing-Windows-Servers-and-VMware-Virtual-Machines.pdf
18. P. S. Murthy and V. Nagalakshmi, "Database Forensics and Security Measures to Defend from Cyber Threats," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1302-1307, doi: http://dx.doi.org/10.1109/ICISS49785.2020.9316042
19. Ramesh, G., Logeshwaran, J., & Aravindarajan, V. (2022). A secured database monitoring method to improve data backup and recovery operations in cloud computing. BOHR International Journal of Computer Science, 2(1), 1-7. https://doi.org/10.54646/bijcs.019
20. Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. https://wjarr.com/sites/default/files/WJARR-2024-1727.pdf
21. Luca Bertolaccini, Pierre-Emmanuel Falcoz, Alessandro Brunelli, Hasan Batirel, Jozsef Furak, Stefano Passani, Zalan Szanto, The significance of general data protection regulation in the compliant data contribution to the European Society of Thoracic Surgeons database, European Journal of Cardio-Thoracic Surgery, Volume 64, Issue 3, September 2023, ezad289, https://doi.org/10.1093/ejcts/ezad289
22. Naeem, M. et al. (2022). Trends and Future Perspective Challenges in Big Data. In: Pan, JS., Balas, V.E., Chen, CM. (eds) Advances in Intelligent Data Analysis and Applications. Smart Innovation, Systems and Technologies, vol 253. Springer, Singapore. https://doi.org/10.1007/978-981-16-5036-9_30