International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 04 | Apr 2025 www.irjet.net p-ISSN: 2395-0072

A Review of Advanced Database Security: Mitigating Cyber Threats and Access Control Mechanisms

Mohd Adeel Ahtram[1], Deepshikha[2]

[1]*Master of Technology, Computer Science and Engineering, Lucknow Institute of Technology, Lucknow, India*
[2]*Assistant Professor, Department of Computer Science and Engineering, Lucknow Institute of Technology, Lucknow, India*

Abstract - *Owing to the fast expanding data driven technologies and the ever growing dependence on databases in industries, database security has become a key issue in cybersecurity. In this review paper, we review advanced database security landscape, aimed to improve its security with mitigation strategies in case of cyber threats, and enhanced access control mechanisms. With advanced, state of the art cyberattack on a rise, SQL injection, data breaches and insider threats, traditional security measures are no longer sufficient. The provenance analysis that we presented in Section 6 can fully integrate with cuttingedge techniques such as encryption methods, intrusion detection and prevention systems (IDPS), database activity monitoring (DAM) and integration of blockchain technology for ensuring data integrity. Furthermore, it looks into modern access control mechanisms like Role based access control (RBAC), attribute based access control (ABAC) and fine grained access control and also discusses the pros and cons of each access control mechanism. Some emerging trends that are discussed include the implications of quantum computing, application of artificial intelligence (AI) and machine learning (ML) for predictive threat analysis, and challenges of securing database in cloud and edge computing environments. Key challenges are: security performance trade off, scalability, compliance in terms of data protection, etc. This review is meant to present a roadmap for researchers and practitioners on developing robust, adaptive, and future-proof database security solutions through synthesis of the recent advancements and discussion on the open issues. Finally, this paper highlights the constant need for innovation and team work to counteract emerging threats in cyber space keeping the critical data in this space secure, available and with integrity.*

Key Words: Database Security, Blockchain for Data Integrity, SQL Injection, Data Breaches, Artificial Intelligence in Cybersecurity, Cloud Database Security.

1.INTRODUCTION

1.1.Background

Modern computer systems are built upon databases as the main storage, management, and retrieval of important data from industries ranging from finance and healthcare, to e-commerce and government. However, their ability and responsibility in data driven decision making, business operations and innovation cannot be stressed any further. With more data being generated and processed at even higher speeds, however, databases have become a favored target of cybercriminals.

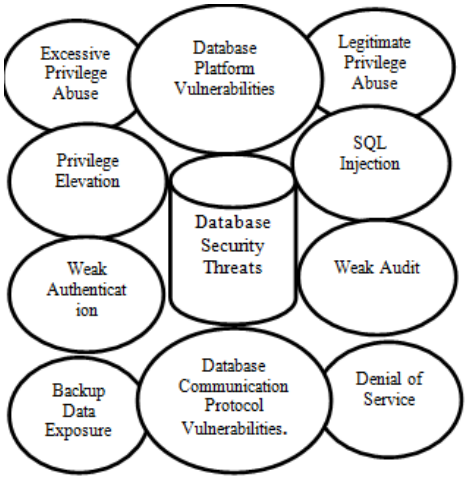

Figure-1: Database Security Threats

Traditional database security measures have been exposed for the vulnerabilities they are in the presence of increasing frequency and sophistication of cyber threats such as SQL injection, data breach, ransomware attacks and insider threats. In addition to the detrimental impact on the confidentiality, integrity, and availability of sensitive information, these threats bring massive financial losses, reputational damage, and lawsuits against organizations. Need for stronger security measures is specially required at this time. The main focus of this paper is to address these challenges by looking into recent research techniques and mechanisms designed to protect database against evolving cyber threats.

1.2.Objectives of the Review

In short, the main goal of this review is to summarize in detail these techniques that expand the database security with their efficiency in defense of cyber threats and boosting the access control techniques. The paper specifically looks into innovative approach like encryption,

intrusion detection and prevention systems (IDPS), and blockchain technology, which radically changes the current approach towards database security. Moreover, it attempts to assess the use of modern access control mechanisms such as Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) to determine their capabilities and shortcomings in securing sensitive data. With the synthesis of recent research and real-world cases, this review hopes to provide useful insights towards researchers, practitioners and policymakers that care to fortify database security amid an increasingly interwoven and data oriented world.

1.3.Scope of the Paper

In this paper, recent database security advances are discussed (cyber threats and an improvement in access control mechanisms are taken). Security in aspect of databases is considered in both theoretical and practical way, focusing also on emerging technologies prone to affect the database security greatly, like the artificial intelligence (AI), machine learning (ML) and quantum computing. Although the review covers a wide variety of topics, the focus is especially on techniques and strategies that can be applied directly to mitigate cyber threats and provide strong access control. It will also cover issues like trade off between security and performance, compliance with data protection regulations and the human factors contributing to security vulnerability.

2.OVERVIEW OF DATABASE SECURITY

2.1.Importance

Security of database means the set of measures, tools and protocols used for protection of the databases against the unauthorized access, misuse, corruption or theft. It consists of very wide range of practices to ensure that the sensitive information is confidential, in intact and accessible only to authorized users only. The database security is the integral element of the database cybersecurity. This is especially true in today's times of digital age, where data is key for the business operations of organizations. A compromised or a breach of a database could result to a lot of severe consequences including financial losses, legal liabilities and damage to an organization's reputation. The stakes are even higher for industries that store sensitive personal and organizational data like healthcare, finance, and government. Database security is not only a technical necessity but it is also a business imperative and is essential for customers' trust, regulatory compliance and smooth operation of the business.

Figure-2:Cyber mitigation steps

2.2.Key Components of Database Security

Confidentiality, Integrity, and Availability form the base of database security. Confidentiality makes sure that sensitive information is only available to the authorized people and it can be ensured by encrypting data and access control mechanisms. Integrity ensures that the data is neither altered nor modified by anyone without authorized and correct purposes. Availability guarantees that the data is accessible to users with appropriate rights when it is required — for instance, protected against a denial-of-service (DoS) attacks or hardware failure. Once we go beyond the CIA triad, database security also comprises three critical processes; these are to be listed as Authentication, Authorization, and Auditing. Authentication proves the identity of users trying to access the database usually by using a password, biometrics or multi factor authentication (MFA). Authorization is applied at the level of authenticated users in order to grant them access within a limited scope. Auditing is about tracking & logging of database activities so that during incidents I can investigate them and suspicious activities can be detected and security policies can be followed. Together, these create a solid framework for protecting databases from many threats.

2.3.Evolution of Database Security

Now although, over the decades, the field of database security has grown as the complexity of data has grown and complexity of cyber threats has grown also. Database security in the early days of computing was comparitively simple, revolved round physical security and basic access controls. Over time, unto databases became more essential to the operation of business, and along with that, more advanced forms of security built up to meet the demand. Networked systems brought new vulnerabilities, which necessitated the creation of encryption protocols, firewalls, and intrusion detection systems to address the vulnerabilities. Over the past few years, the prevalence of cloud computing, big data, and Internet of Things (IoT) has only served to accelerate the complexity of the security landscape, and the recent emergence of machine learning

based threat detection, blockchain for data integrity, and zero-trust architectures has only indicated how entirely it has evolved in the recent past. This is typical of the transition from traditional to advanced security measures that occur in the ongoing arms race between cyber defenders and attackers as it necessitates constant innovation and adaptation in database security methods.

3.CYBER THREATS TO DATABASES

3.1.Types of Cyber Threats

In this enterprise, cyber threats aimed mainly on databases increase noticeably, which pose specific problems to the security of databases. SQL Injection is one of the most common and dangerous threat that an attacker can exploit the vulnerability in a web application to inject a malicious SQL Query to a database. This enables them to get sensitive data from or manipulate it without detection. Denial of Service (DoS) attacks, namely when database servers are overwhelmed with too many requests, effectively making them inaccessible to legitimate users and hindering business operations, is another major threat.

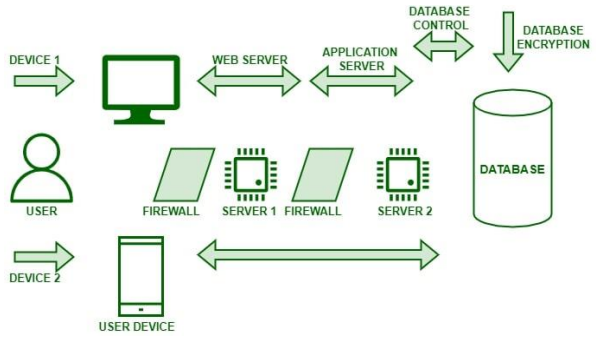

Figure-3: Working of Cyber Threats to Databases

Malicious or negligent employees with access to the database are also a serious insider threat, able to be purposely or inadvertently put data at risk. Furthermore, malware and ransomware attacks are more and more frequent, and attackers employ malicious software that encrypts or steals data in order to demand ransom in exchange for the release of the data. Data breaches and exfiltrate where unauthorized access to databases leads to the theft or leakage of sensitive information is the last. This demonstrates the various and changing risks relevant to modern databases.

3.2.Impact of Cyber Threats

Cyber threats to databases can have devastating consequences to organizations. Financial losses are a most immediate impact—many breaches directly cause theft, ransom, or even the costs of investigating and fixing a problem. Organizations suffer monetary damage beyond anything else, but the damage to their reputation comes as customers and other stakeholders no longer trust that their information is safe. If trust is lost, then the business would also come down, the clients would start taking their business somewhere else. Additionally, organizations suffer legal and regulatory ramifications due to data breaches as they typically run afoul of activities like the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA). The other associated costs are also huge as non compliance even can lead to hefty fines, lawsuits and in some cases mandatory audits. The combined body of consequences makes it necessary to establish tight database security.

3.3.Case Studies

For instance, real world examples of database breaches can shed light on the world of cyber threats in nature and behavior. One of the most known cases of online exploitation happened in 2017 when Equifax had to admit that hackers had managed to hack the personal data of none less than 147 million individuals, when they used vulnerability in the company's web application. It severely damaged the reputation, finances, and led to legal consequences for Equifax in the end. For instance, the 2013 Target breach resulted from attackers getting into the company's database via third party vendors, compromising the credit card information of 40 million customers. This incident brought the danger of being vulnerable throughout the supply chain, as well as securing access points to the access to the database home. This was similarly exemplified by the 2021 attack on the Colonial Pipeline through a ransomware attack which both shut down the operational pipeline and resulted in significant business impact and financial losses for the company. These examples reveal the extent of damage database breaches can cause and some of the efforts that must be taken moving forward to protect us all from future incidents of this kind. These incidents have taught us about the critical role of timely vulnerability patching, strong access control and consistent monitoring to detect and respond to threats.

4.ACCESS CONTROL MECHANISMS

4.1.Role-Based Access Control (RBAC)

Access control mechanism widely used is Role Based Access Control (RBAC), which assigns permission to users according to the role in an organization. In this model, a role is imposed according to function of the job, and that role is provided certain rights to access database resources. For instance, a manager might be granted access to financial data where as an employee may only see general operational data. With RBAC, you assigned users in groups of roles and then simplified permissions control. On the other hand, it is scalable, easy to administer, and is better able to comply with security policies. RBAC suffers from limitations, including its

rigidity in dealing with the dynamic and context sensitive requirements for access. For example, it may not be suitable for cases in which temporary or conditional access is required. While these limitations are well known, RBAC remains the main access control approach in many organizations.

4.2.Attribute-Based Access Control (ABAC)

The Attribute Based Access Control (ABAC) is a more flexible and dynamic access control model where the evaluation of the user access request is done based on a combination of attributes. Some of these attributes could be user characteristics (e.g., job title, department), resource properties (e.g., sensitivity level, ownership), environmental conditions (e.g., time of day, location). ABAC determine access should be allowed by using policies, and hence it is highly customizable to meet complex and varied security demands. For instance, in a policy, a user may be allowed to access a database as long as the user is in a particular department and at a certain time of the day. Modern databases that accesses are dynamic and context dependent, for example in cloud settings or in multi tenant systems, these are precisely the situations where ABAC is of great use. However, this flexibility comes at the expense of increased policy definition and management complexity which is challenging to organizations.

4.3.Mandatory Access Control (MAC) and Discretionary Access Control (DAC)

There are two different ways for access control, namely Mandatory Access Control (MAC) and Discretionary Access Control (DAC). MAC is a strict model in which access decisions at the instance of an access control point are made by a central authority on the basis of well defined security labels and policies. MAC is highly secure, because user cannot alter access permissions, but also inflexible. This is generally considered for the environments where confidentiality levels are very high and are suitable for government or military systems. On the other hand, DAC grants more freedom to resource owners regarding who to allow access, while it is less centralizing. DAC is easier to implement and manage, but it is more prone to misuse or errors due to an accidental grant of too many permissions by the users. The decision between MAC and DAC is a matter of these security requirements and related operational context of the organization. Sometimes, a middle of the road approach is taken adopting features from both models to match security with flexibility.

4.4.Multi-Factor Authentication (MFA)

One of the most important elements of modern access control is Multi-Factor Authentication, which is meant to improve the security by requesting the user to furnish a variety of proofs of identity when getting access to the database. MFA frequently involves something the user knows a password, something the user has a smartphone or security token and something the user is biometric data like fingerprints or facial recognition. MFA drastically minimises the risk of unauthorised access as it adds extra layers of verification that is even if 1 of the factors (Password) is compromised. It's no surprise, MFA is most successful at preventing credential theft and phishing, the two ways used by hackers to access a computer network's database. MFA only improves security and can introduce usability challenges, like a slower login time and the need to purchase additional hardware. Nevertheless, these inconveniences are more than offset by the security value of MFA, which is why MFA is an established best practice for protecting sensitive databases.

4.5.Fine-Grained Access Control

More Grained Access Control (FGAC) is the strategy used when access restrictions are enforced to a very detailed level, such as on a row or column level of a database. For instance, row level security makes sure that user can see only specific rows of data as per pre defined rules, like their department or geographic location. Column level security, on the other hand, limits data access only to certain columns, for instance, for columns that contain private or financial information.

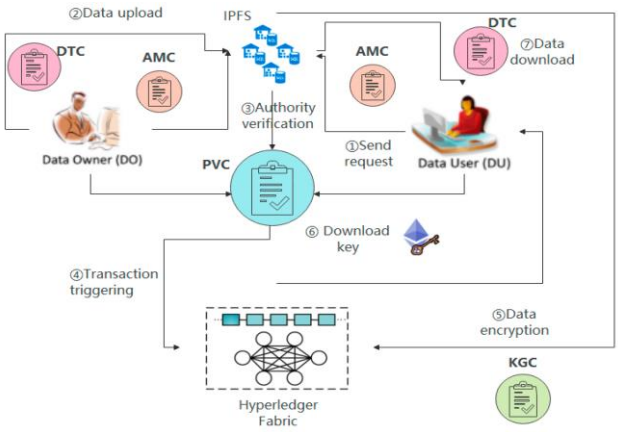

Figure-4: Fine-Grained Access Control (FGAC)

In particular, situations where various levels of user or group require access for a subset of data within an identical database are where FGAC is most effective. Nevertheless, implementing FGAC is difficult because of the complexity of access policies design and its integration with the existing database systems. However, issues like supporting performance, scalability, and ability to handle policy update exist. However, in spite of these challenges, FGAC is a strong tool for reducing data exposure and security enhancement in scenarios where diverse access is needed. These implementation challenges are increasingly being addressed with solutions like policy based

frameworks as well as advanced database management systems.

5.EMERGING TRENDS AND FUTURE DIRECTIONS

5.1.Artificial Intelligence and Machine Learning in Database Security

The artificial Intelligence (AI) and Machine Learning (ML) tools are changing the database security field by providing the predictive threat analysis, and automated response tools. These technologies are capable of processing large volumes of data and spotting the pattern and anomalies that could indicate a potential cyber threat. For example, ML algorithms can identify unexpected access patterns or abnormal queries that are out of the ordinary and alert on these things as something to investigate further. Historical data and real time monitoring is utilized by the predictive threat analysis to predict and mitigate risks before happening which can be referred to as database security on a pro active basis. In addition, an automated response system driven by AI can respond almost immediately to any detected threat, for example blocking malicious users, isolating compromised computers and applying patch for the vulnerabilities. These capabilities are not just more efficient when it comes to what is required of security operations, but they also reduce the amount of human involvement that would have a chance of human error. With AI and ML advancing, the integration of these technologies into the database security frameworks will also become more complex, ensuring that threats will be more safeguarded.

5.2.Quantum Computing and Its Impact on Database Security

Although quantum computing is, certainly, in its infancy, it presents as one opportunity, as well as one challenge for database security. Quantum computers have the potential to solve complex problems at a speed never known before; this could be applied to enhance the encryption and security algorithms. At the same time, they also represent a strong threat to currently existing cryptographic systems. Currently, there is a large number of encryption algorithms, such as RSA and ECC, that need to factor a large number or solve a discrete logarithm problem, which are the ones which Quantum Computers can solve in an efficient way using algorithms such as Shor's algorithm. This enables sensitive data to be exposed to unprecedented risk, potentially making traditional encryption methods obsolete. To overcome this, researchers develop quantum resistant algorithms which are based on lattice based cryptography and hash based signatures that can be resistant to quantum attacks. Database security in the coming years will be a critical focus on the transition to quantum resistant encryption, which will require the active participation of researchers, industry and policymakers to make a smooth, secure transition.

5.3.Privacy-Preserving Data Sharing

We are at an inflection point in data sharing, where collaboration and innovation are increasingly driven by sharing our insights with others but we also have to be able to offer our valuable information to only those we trust (i.e. ensuring privacy). In this area, there are two important approaches: differential privacy and secure multi party computation. It is a method to protect a dataset by adding noise to your dataset so personal identifying faculties from your people aren't unveiled, and you nonetheless get to get significant info from the dataset. Since it enables individual privacy to be preserved in situations where data will be shared with other parties, not only researchers but also business partners, for example, this is a very useful technique. Secure multi party computation (SMPC), however, allows multiple parties to jointly compute a function on their inputs without being able to see the inputs. It allows collaborative analysis and decision making with the underlying data remaining confidential. Nevertheless, these approaches are catching on in areas like healthcare, finance and government as its sensitivity to data is paramount. It will be crucial for these techniques to play a role in the enabling of privacy for privacy regulations that are becoming more stringent.

5.4.Integration with Cloud and Edge Computing

The move towards cloud and edge computing creates new security problems for databases, especially in the distributed environment is the shift. Scalable, flexible and cheap, cloud databases also bring data to risk of wrong access, data breach, and misconfiguration. Compound this by the fact that edge computing means spills of data to multiple places, increasing the attack area. Organizations respond to these challenges by employing solutions such as encryption in data at rest and in transit, the best identity and access management (IAM) systems, and monitoring tools. In a hybrid and multi cloud environment where data lives across multiple cloud providers, the measures of consistency and security need to reach beyond the boundaries. Recently, emerging techniques that involve data fragmentation (splitting the data and storing it in different locations) as well as federated learning (performing decentralized model training without the need to share raw data) prove to be effective approaches to the protection of distributed databases. Increasingly these cloud and edge computing is gaining momentum and therefore integrating these solutions in database security framework will be crucial for upholding data integrity and confidentiality.

6.CHALLENGES AND OPEN ISSUES

6.1.Balancing Security and Performance

A very significant problem in database security is the delicate balance between secure, robust security mechanisms and acceptable system performance. Even though encryption is very much necessary while securing any sensitive data, it can result in extra latency and lower query processing speed. For instance, encrypting data-at-rest and data-in-transit provide confidentiality but the computational overhead for the encryption and decryption process slows down the database operation. Like, either by implementing advanced security mechanism like intrusion detection system or fine grained access control you can make your database system complex as complex system and more resource consuming which in turn can degrade the overall performance of your database system. These tradeoffs are challenging for organizations to carefully evaluate and must optimize their security configurations to minimally degrade performance in order to provide enough security. This challenge was addressed with techniques such as selective encryption where only the most sensitive data is encrypted, or the use of hardware based acceleration for cryptographic operations to minimize the computational overhead. However, reaching such an optimal balance is still a problem, especially in an environment involving high performance or real time database.

6.2.Scalability of Security Mechanisms

As databases become larger and more complicated, scalability of security mechanisms becomes an important issue. Big data analytics, cloud environments, and such large scale databases handle large amounts of data and serve large number of concurrently accessing users. Such environments tend to put enormous demands on traditional security measures, which were shaped for smaller two tier, centralized systems. Take, for example, access control systems that need to deal with rapid growth in terms of permissions for millions of users, or encryption techniques that have to perform the encryption and decryption of petabytes of data; additionally, we need performance to be as high as possible with as little bottleneck as possible. In addition, monitoring and auditing tools must be responsive to such high volume of log data in real time in order to detect and react to threats. All this is further exacerbated in distributed databases where the data is distributed over multiple nodes or locations. The solutions to these issues often involve inventing new techniques such as distributed encryption protocols, scalable access control frameworks, and machine learning based monitoring system which are able to cater to the evolving requirements of large databases.

6.3.Human Factors in Database Security

One shouldn't discount the human factors when security is concerned; they play an equally important role as technological solutions for the database security. It is also possible that employees, contractors and other insiders with access to databases inadvertently or worse intentionally, compromise security by following poor or weak password practices, falling prey to phishing attacks, or misconfiguring security settings. One of the hardest risks to mitigate are insider threats, which are defined as whether malicious or accidental, they actually are trusted individuals with legitimate access to sensitive data. These issues can be dealt with by training and awareness programs educating the users about the security best practices along with the disadvantage of negligence. Along with that, organizations must enforce strict access control policies, track user activity for any unusual behavior, and promote a security awareness culture. Preventive security measures include techniques like role-based training, simulated phishing exercises, and performing security audits on a regular basis to prevent errors from humans and by insiders. In the end, getting the databases holistically secure entails employing technological tools and approaches as well as human approach centered ones.

7.CONCLUSION

In this review paper, the green area of advanced database security covers its mechanism and techniques of counter threat and access control. For instance, key findings make it clear how any encryption methods, such as data-at-rest encryption and data-in-transit encryption, are essential to keep sensitive information secure from unauthorized access. Intrusion detection and prevention systems (IDPS) and database activity monitoring (DAM) have advanced tools that are essential to identifying and responding to threats in real time. Moreover, modern access control methods (role based access control (RBAC), attribute based access control (ABAC), and fine grained access control) can be used to provide flexibility and scalability in managing user permissions.

The dynamic nature of cyber threats necessitates a commitment to continuous improvement in database security practices. Organizations need to do so in order to remain ahead of such potential risks as attackers continue to develop more sophisticated methods. This involves regular upkeeping of security protocols, adopting leading edge technologies, and cultivating a hackable environment in the name of innovation, communication and collaboration within the cybersecurity community as a whole. For example the integration of AI and ML to automate the detection and response of threats, presents a fantastic opportunity but also needs to continually evolve to adapt to new vectors of attack. Likewise, continued research and development toward quantum resistant encryption as well as the use of privacy preserving

techniques will be necessary. In addition, the scalability and performance optimization of these organizations must also be taken into account so that the security measures do not overshadow the performance and the functionality of large or high performance databases. Oftentimes, when adversity strikes, organizations fall prey to the 'taker' mentality, where crawl, walk, run becomes characterized as survival.

REFERENCES

1. A. Shostack, Threat Modeling: Designing for Security, Wiley, 2014, doi: 10.1002/9781118810057.

2. R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed., Wiley, 2008, doi: 10.1002/9781118820872.

3. M. Bishop, Introduction to Computer Security, Addison-Wesley, 2004, doi: 10.5555/1076264.

4. J. Katz and Y. Lindell, Introduction to Modern Cryptography, 2nd ed., CRC Press, 2014, doi: 10.1201/b17668.

5. N. Provos and D. Mazieres, "A Future-Adaptable Password Scheme," in Proceedings of the 1999 USENIX Annual Technical Conference, 1999, doi: 10.5555/1267303.1267305.

6. R. S. Sandhu and P. Samarati, "Access Control: Principles and Practice," IEEE Communications Magazine, vol. 32, no. 9, pp. 40–48, Sep. 1994, doi: 10.1109/35.312842.

7. D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST Standard for Role-Based Access Control," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 224–274, Aug. 2001, doi: 10.1145/501978.501980.

8. V. C. Hu, D. Ferraiolo, R. Kuhn, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute-Based Access Control (ABAC) Definition and Considerations," NIST Special Publication 800-162, Jan. 2014, doi: 10.6028/NIST.SP.800-162.

9. E. Bertino, R. Sandhu, and B. Thuraisingham, "Database Security—Concepts, Approaches, and Challenges," IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 1, pp. 2–19, Jan.-Mar. 2005, doi: 10.1109/TDSC.2005.4.

10. A. Kamra, E. Bertino, and R. Terzi, "Detecting Anomalous Access Patterns in Relational Databases," The VLDB Journal, vol. 17, no. 5, pp. 1063–1077, Sep. 2008, doi: 10.1007/s00778-007-0063-0.

11. C. Dwork, "Differential Privacy," in Proceedings of the 33rd International Conference on Automata, Languages and Programming (ICALP), 2006, doi: 10.1007/11787006_1.

12. O. Goldreich, Foundations of Cryptography: Volume 2, Basic Applications, Cambridge University Press, 2004, doi: 10.1017/CBO9780511721656.

13. M. Abadi, A. Chu, I. Goodfellow, H. B. McMahan, I. Mironov, K. Talwar, and L. Zhang, "Deep Learning with Differential Privacy," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS), 2016, doi: 10.1145/2976749.2978318.

14. P. Rogaway, "The Moral Character of Cryptographic Work," Cryptology ePrint Archive, Report 2015/1162, 2015, doi: 10.13140/RG.2.1.4296.9445.

15. M. A. Khan and K. Salah, "IoT Security: Review, Blockchain Solutions, and Open Challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, May 2018, doi: 10.1016/j.future.2017.11.022.

16. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

17. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," in 2015 IEEE Symposium on Security and Privacy (SP), 2015, doi: 10.1109/SP.2015.14.

18. M. N. Islam, M. S. Hossain, M. F. Hasan, and M. A. Rahman, "A Survey on Database Security: Threats, Countermeasures, and Challenges," International Journal of Computer Applications, vol. 180, no. 6, pp. 1–8, Jan. 2018, doi: 10.5120/ijca2018916438.

19. A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, Jun. 2006, doi: 10.1109/TIFS.2006.873653.

20. Y. Lindell and B. Pinkas, "Secure Multiparty Computation for Privacy-Preserving Data Mining," Journal of Privacy and Confidentiality, vol. 1, no. 1, pp. 59–98, 2009, doi: 10.29012/jpc.v1i1.566.

21. G. McGraw, Software Security: Building Security In, Addison-Wesley, 2006, doi: 10.5555/1196896.

22. B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., Wiley, 1996, doi: 10.5555/519939.

23. M. Bishop, "Computer Security: Art and Science," Addison-Wesley Professional, 2002, doi: 10.5555/580876.

24. E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018, doi: 10.17487/RFC8446.

25. A. Juels and R. L. Rivest, "Honeywords: Making Password-Cracking Detectable," in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS), 2013, doi: 10.1145/2508859.2516671.

26. M. Abadi, M. Burrows, M. Wobber, and P. W. Manber, "Moderately Hard, Memory-Bound Functions," ACM Transactions on Internet Technology, vol. 5, no. 2, pp. 299–327, May 2005, doi: 10.1145/1064340.1064341.

27. R. Canetti, "Universally Composable Security: A New Paradigm for Cryptographic Protocols," in Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science (FOCS), 2001, doi: 10.1109/SFCS.2001.959888.