Fall 2022

Data Leaks Detection Mechanism for Small Businesses

Hannan Mohammed Abdul

Need of Data Leaks Detection Mechanism for small businesses in Modern World

By

Hannan Mohammed Abdul

B.E. E.C.E Osmania university, 2019

THESIS

Submitted in partial fulfillment of the requirements

For the Degree of Master of Science,
With a Major in Information Technology

Governors State University
University Park, IL 60484

2022

Abstract

The protection of sensitive customer information is a vital responsibility for companies of all sizes. In modern times, there is a significant need for not only protecting the data that is being shared but also gaining knowledge of its leakage points and the circumstances under which it is compromised. After locating the location where data is being lost, it is necessary to identify the person responsible for the breach. When it comes to protecting a company from suffering significant financial damage because of data leakage throughout the course of normal business operations, it is very essential to have a solid understanding of the individuals who are responsible for leaking the data. This study tries to discover how small firms might be assisted in protecting the sensitive information that they own. This study's objective is to determine how sites of companies react to attacks that are damaging to their operations so that appropriate action may be taken.

1. Introduction

Data plays a significant part in the performance of main tasks of today's commercial operations in the contemporary world, which has seen significant technical improvements in recent decades. Data leakage refers to the communication of private or sensitive information or data from a business to an unknown third party without the company's knowledge or consent. In most situations, it is a case of an unauthorized receiver. One seemingly little data breach might result in the closure of an entire company or a significant financial loss for the operation as a whole in today's hyper-advanced business environment, where companies are so well-equipped to handle their customers' information.

Depending on the kind of business or industry, the company's data may include sensitive personal credit card information, health records, trade secrets, and other types of information as well. Even if the information shifts often from one point in time to the next, the data that pertains to a particular time has its own significance, and as such, it must be protected and monitored by certain authentications while it is being transferred through one party to another. If the information were to leak while it was being transferred to an unauthorized third party, then it would be of the utmost importance to determine how the leak occurred and who was accountable for the leakage. This would allow the guilty party to be identified and punished, as well as ensure that any additional data or information would be adequately protected in the future.

The most recent edition of Verizon's Data Breach Investigations Report indicates that the number of ransomware assaults has increased by 13 percent over the course of the previous year. This is greater than the sum of the increases seen over the previous five years combined (DBIR). Today, May 24, sees the release of the 2022 edition of the Data Breach Investigations Report (DBIR), which analyzed almost 24,000 data leakages, of which 5,212 were confirmed data leakages (2022 Data Breach Investigations Report, 2022). The goal of cybercriminals is to acquire financial gain, celebrity, personal vengeance, or to disrupt organizational functions by gaining access to secret information and either modifying or deleting it. To carry out their assaults, these attackers take advantage of software vulnerabilities, the excessive workload and inexperience of personnel, and the variety of security solutions that have been installed in a business. In this setting, businesses need to adopt techniques that enable them to remain resilient in the face of harmful assaults so that they may continue functioning normally (Ping et al., 2016). The use of security mechanisms results in the creation of additional layers of protection and the generation of event logs that can be investigated to identify and respond to potential invasions (Ghafarian, 2017). In this paper, I want to find the ways that can help small businesses in shielding their crucial information. The purpose of this study is to identify methods through which businesses' sites respond to assaults that are detrimental to their operations.

2. Literature Review

The term "data leakage" or "information leakage" refers to the unintentional movement of data from inside an organization to a destination or container located outside of the company (e.g., flash drive, and CD). Data may be purposefully or maliciously leaked using either an electronic or a physical approach by an insider or an outsider in the firm. Security analysts are required to regularly monitor the security logs of a variety of systems and resources, looking for signs of information breaches in large amounts of data, so that they may spot potentially malicious activities. The exploitation of vulnerabilities is often the cause of information leaks, which may originate from either an external or an inside source. Code injection attacks are a subset of a larger class of attacks that depend on the practice of injecting data into a web application in order to either execute malicious data in an unexpected manner or interpret legitimate data in an unexpected manner (Singh, Dayal, Raw & Kumar, 2016). Injection assaults are the most popular and effective sort of attack on the Internet. This is due to the different varieties of injection attacks, the huge attack surface they provide, and the complexity that is often necessary to prevent them. Failures in injection occur if untrusted data are supplied to an interpreter as part of a command or query. The attacker's malicious data may trick the interpreter into carrying out instructions it wasn't supposed to or accessing data it shouldn't have. SQL injection is a common attack technique that's used by hackers (Ghafarian, 2017). SQL injection is popular among cybercriminals because of the flexibility it offers. It is possible to use it to steal client information, change or delete private data, and gain total control of a website by using it in these ways (Voitovych, Yuvkovetskyi & Kupershtein, 2016). Furthermore, it is not always simple to see. Even if an application is able to properly sanitize user input and thwart an immediate assault, the tainted data will still be kept locally, and it may cause havoc if it is utilized in a different context in the future (Yunus et al., 2018). A cursory examination of the relevant literature suggests that a powerful mechanism in conjunction with adequate training may aid businesses in recognizing and preventing these assaults. Encryption, to provide one example, is a method that may make the data more secure. The plain text of anything like an email or text message is encrypted and then converted into ciphertext, which is a format that cannot be read by humans (Ping et al., 2016). This contributes to the protection of the secrecy of digital data, whether it be data that is kept on computer systems or data that is transported across a network such as the Internet. When the person to whom the communication is addressed accesses the message, the information is converted back to its initial state. Encryption is the term used for this process. A "secret" encryption key is a set of techniques that can scramble and unscramble data back to a readable format. To decipher the message, both the sender and the receiver will need to utilize the key. The staff may be better prepared to ward against assaults carried out through social engineering or phishing by participating in a training program that can assist in this endeavor (Qian et al., 2015).

2.1 Data Leak & Data breach:

In recent years, there have been many high-profile data breaches and leaks, which have drawn a lot of attention to the topic of cyber security. A data leak occurs when sensitive data is released to the public inadvertently, while a data breach is an incident that takes place because of a cyberattack. A software misconfiguration that makes it easier for unauthorized users to get access to critical resources is an example of a data leak. This kind of data loss occurred in 2021 with the significant Microsoft PowerApps data breach (Cheng, Liu & Yao, 2017).

The circumvention of network security restrictions by a cybercriminal to get access to sensitive resources is an example of a data breach. These kinds of cyber-incidents are happening more often, and there are a lot of cases that back up this assertion (Howard &

Gulyas, 2014). Both data leakage and data breaches ultimately result in the same thing, which is the compromising of sensitive data. The drive that led to the achievement of this goal is the fundamental factor that sets these two occurrences apart from one another (Fleury-Charles, Chowdhury & Rifat, 2022). The next section of the paper covers the topic of data leaks as well as data breaches in further depth.

2.1.1 Data Leak:

Most of the time, insufficient security methods are to blame for lost or stolen data. If one of a company's suppliers has a data breach, the company might also be negatively affected. It is difficult to discover and remedy these vulnerabilities in a timely manner before it is too late. This is because they are spread out across a large attack landscape. If organizations do not implement a comprehensive data security solution, they will continue to be susceptible to data breaches caused by their third-party networks.

2.1.2 How data leakage occurs:

There are a lot of different ways that data might get out. The three potential scenarios for data leaking are described in the following paragraphs. The first possible scenario involves the accidental disclosure of data. A genuine user made a mistake and exposed sensitive data, which was then sent in the outgoing traffic. The purpose of this research is to propose a method for identifying the kind of inadvertent data breaches that occur across a network. Accidental disclosures of sensitive information can occur for a variety of reasons, including human error (such as forgetting to use encryption) or application flaws (such as carelessly forwarding an internal email and its attachments to outsiders). Both of these scenarios are examples of inadvertent data leaks (Papadimitriou & Garcia-Molina, 2009).

The second kind of data leaking is one that was done on purpose. A hostile insider or piece of software that is both malevolent and covert might take sensitive personal or corporate data from a host in these kinds of situations. This kind of leak is outside the capabilities of our network-based solution since the hostile opponent may block content-based traffic inspection by using strong encryption or steganography (Verma et al., 2020). As a result, this kind of leak is not covered by our solution. Instead, it is necessary to implement host-based defenses, such as identifying the virus while it is being spread.

The third scenario involves data transmission that is lawful and intentional. In these kinds of situations, the sensitive data is sent by a legitimate user with the intention of being used for a valid purpose. In this article, we use the assumption that valid data transfers make use of data encryption methods such as SSL. This enables one to differentiate genuine data transfers from accidental data leaks (Yunus et al., 2018). As a result, it is reasonable to conclude that unencrypted sensitive material appearing in network activity is the result of data breaches that occurred by accident.

A simple example of data loss may be shown in picture 1. In this scenario, the business owner accomplishes his goal by entrusting his trustworthy agents with the responsibility of managing the company's data files. However, as time passes, one of those agents betrays the business owner's confidence by disclosing shared information to an unauthorized third party. The phrase "data leakage" refers to the process by which proprietary company information is obtained by a third party without the knowledge or consent of the data's owner (Zuo, Lin & Zhang, 2019). The social networking sites of today, such as Facebook, Twitter, and others, along with

Through their third-party apps, everyone is utilizing a portion or all the personal information of their users, which they pledge to keep confidential and safe. And there will always be the possibility that the personal information of users may become public, and when that happens, it will be required to identify the individual responsible for the leak and ensure that users' information is kept secure in the future. The future of any user's private information always requires that it be protected but have no leaks to unauthorized individuals who can miss utilize the data to any degree (Gomez-Hidalgo et al., 2010). This is because unauthorized people have the potential to misuse the data in any manner.

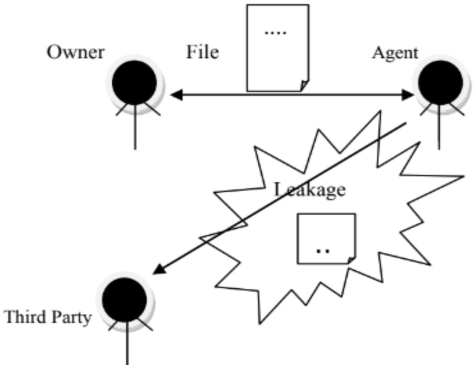

Figure 1: ***Data Leakage***

2.2 Data Breach:

A data breach is the result of an intentional cyber assault, while a data leak is the unintentional disclosure of sensitive data by a company. A data breach is a serious matter. Cybercriminals do not generate data leaks; rather, they find them and utilize them to execute data breach attacks once they have found them (Saleem & Naveed, 2020).

The precise type of data breaches will differ from sector to sector, organization size to organization size, and network design to network infrastructure. On the other hand, the most fundamental definition of a data breach is the illegal access to digital information that would normally be considered private (Thomas et al., 2017). The illegal nature of cybercriminals' personal information that does not belong to them is the most important factor to consider in this context. What cybercriminals do with the data might vary widely depending on their goals. The exfiltration of information that malicious actors have access to but shouldn't or data that actors have access to but do not have specific authorization to disseminate may also be considered a violation of data security (Singh, Dayal, Raw & Kumar, 2016).

Although there are many various kinds of data breaches, there is a pattern that can be identified in every one of them. This is an interesting fact, and it's important to note that they follow a predetermined pattern. Cybersecurity teams are able to better evaluate one ‘s own threats and risks and start preparing defense systems to make it too nearly impossible for the majority of cybercriminals to successfully penetrate by conducting an analysis of the most common steps that malicious hackers may start taking on their way to attempting to pull off an effective security breach (Saleem & Naveed, 2020).

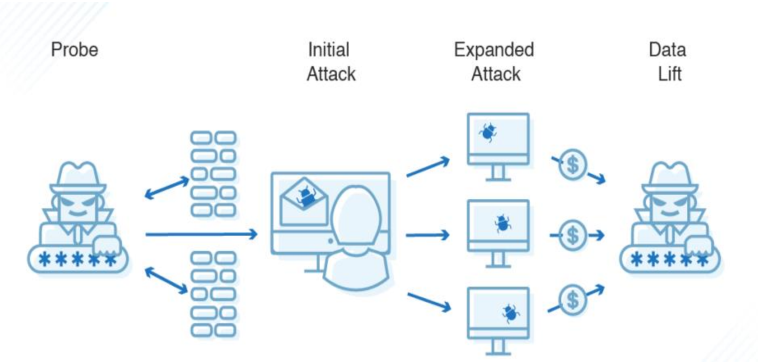

Figure 2: ***Data Breach***

2.1.2 How data breach occurs:

The first step of these kinds of assaults is called the probe. At this point, malevolent actors start to learn more about both the network and the wider digital world they are operating in. They may test the cybersecurity defenses, examine how to start a potential phishing email, test passwords, or hunt for outdated software that lacks the most recent security updates (Sun, Xu & Zhao, 2021).

The first assault constitutes the second phase. When the attackers have a good idea of how to carry out the attack most effectively, they will launch the first wave of their assault. This may involve sending an email to employees in which an attempt is made to trick them into clicking on a link that takes them to a malicious website, or it may involve corrupting an application that is essential to the workflows of employees (Mills & Harclerode, 2017).

The expansion occurs in the third phase. Attack. After a weakness has been compromised in this fashion, thieves will consider what course of action to take next. In most cases, this will include them using whatever foothold they already have in order to launch an assault on the remainder of the network and discover as much sensitive personal information as they can (Liu et al., 2018).

The data lift is the very last stage. Because various forms of cyberattacks occur on varying durations, malicious actors may try to extract as much data as possible or may choose to remain quiet until they have a better idea of how much they can get off with (Fang et al., 2021).

2.3 Motivation behind the popular data breach attacks in recent times:

There is not a single business that is safe from cyberattacks, regardless of the level of technical development or the size of the corporation. However, it is important to keep in mind that the kind of information that is taken from a company by an external cybercriminal or an inside bad actor will change from company to company since the individuals who commit these crimes are driven by various goals (Sun, Xu & Zhao, 2021). However, the Verizon analysis revealed that 76 percent of intrusions were carried out for financial gain. This may involve trade secrets, confidential financial data, and sensitive government documents; alternatively, it may center on the theft of customers' personal data, as it has with breaches that have received public attention involving Facebook, Yahoo, and Uber, which cyber attackers could then use for their own benefit. In addition, for HIPAA-covered companies, it is of the utmost importance to be aware of how to avoid security breaches in the healthcare industry; otherwise, the medical records of patients might be compromised (Mills & Harclerode, 2017).

2.4 Popular attacks:

Even the most well-known organizations, like Microsoft and Facebook and Marriott Hotels, may fall victim to a data breach. After years of assaults that grabbed headlines, the communications systems of large organizations are still susceptible to penetration, as seen by the recent breaches at major firms (Biswas et al., 2022).

It was discovered in 2019 that the telephone numbers of about 20% of Facebook users, or 419 million people, had been compromised. It's vital to keep in mind that Facebook itself has not been compromised by hackers. Instead, the databases included information on

Facebook users that had been scraped off the site at a time when Facebook still gave developers access to user phone numbers (Mukhopadhyay, 2022).

Hackers launched an assault on the reservation system used by Marriott in 2018. Marriott International said that unauthorized individuals had gained access to its Starwood reservation system and taken the personal information of as many as 500 million customers. Customers of the hotel had their names, phone numbers, addresses, birth dates, and protected credit card information stolen. Also taken were their email addresses. Additionally, the passport numbers and travel itineraries of a subset of the visitors were collected (Ukwandu et al., 2022).

2.5 Why a business needs to have a mechanism in place to prevent data leakage:

The fact that a single data breach may destroy a company's image is the primary factor that motivates organizations to prioritize the safety of their customers' information. Since the beginning of this decade, each year has been dubbed "Year of the Data Breach," with the number of data breaches increasing steadily year after year. When a security hole is found, there is a flurry of activity on the internet in the form of articles discussing the occurrence, the teams involved, the affected, and the perpetrators of the crime (Singh, Dayal, Raw & Kumar, 2016). One could have the impression that the only bad guy is the cybercriminal who attacked the network, but in reality, they are never the only ones who have to deal with the harsh glare of publicity. If anything, the corporations that fail to secure their customers and their systems are held to an even lower standard of morality than the person who committed the crime. If the hackers are detected, they might face legal consequences (Rode et al., 2020). Companies with security flaws put their reputation at stake. It might be difficult to make up for lost ground when it comes to one's reputation. Research conducted by Centrify found that as a direct consequence of a data breach, 65 percent of victims polled experienced a loss of faith in the affected business, with 27 percent of victims going so far as to sever their ties to the affected organization entirely (Singh, Dayal, Raw & Kumar, 2016).

The second critical part is that it interferes with the continuity of corporate operations. Even the smallest apparently little data loss may cause a disruption to an organization's ability to carry on business as usual, and this is true even when the organization has had a range of data loss events of varying scopes. An employee may mistakenly destroy a crucial file. It is possible for everyone to experience it, and it does so on a consistent basis (Gomez-Hidalgo et al., 2010). It's possible that one day people will go to work, open up the computer, and find a malware text waiting for the person there. Or, one day, when a person is in the middle of a crucial negotiation, the system will be compromised, and the party will lose access to information that is required to successfully complete the transaction. When it comes to transactions in the corporate sector, information is exchanged at least to the same extent as monetary money, if not more so. When people suffer the loss of their data, they go through the 5 levels of grieving (Yaacoub et al., 2022). The continuous operation of businesses is disrupted, and some of those businesses are sometimes forced to shut their doors.

2.6 SQL Injections:

SQL Injection, often known as SQLi, is a kind of injection attack that enables malicious SQL queries to be executed (Ping et al., 2016). These statements are used to operate a database server that is operating in the background of a web application. SQL Injection vulnerabilities allow attackers to circumvent the application security safeguards that are in place. They can circumvent the authentication and permission measures of a website or application and get the complete contents of a SQL database (Qian et al., 2015Z). They also have the ability to employ SQL Injection to add new entries, edit existing ones, or remove old ones from the database.

Any website or online application that makes use of a SQL database, whether it is MySQL, Oracle, SQL Server, or one of the many others, may be susceptible to a SQL Injection vulnerability. Criminals might use it to get illegal access to your sensitive data, including personal data, customer information, intellectual property, trade secrets, and other types of information (Prabakar, KarthiKeyan & Marimuthu, 2013). SQL Injection attacks are among the earliest, most common, and most deadly types of vulnerabilities that may affect online applications. Injections are ranked as the most dangerous threat to web application security in the OWASP Top 10 2017 paper published by the Open Web Application Security (Voitovych, Yuvkovetskyi & Kupershtein, 2016).

2.7 Preventing Data Leakage in Business:

The typical methods used to stop the leaking of sensitive information may be divided into two groups. The first category is solutions based on hosts, while the second category is solutions based on networks. Encrypting data when it is not in use, identifying stealthy malware via anti-virus scanning or monitoring the host, and imposing regulations to limit the transmission of sensitive data are all examples of host-based techniques (Sun, Xu & Zhao, 2021). Encrypting data when it is not in use. These strategies are not mutually exclusive and may be used in conjunction with one another. For instance, the host-based approach mentioned in the storage capsule stops attackers from stealing data from the memory. This protection against data theft involves encryption and data-transfer regulations, in addition to complicated processes for taking snapshots of the whole host. Most host-based solutions need the use of virtualized or specialized hardware in order to guarantee that the detector's system remains intact (Khoei, Slimane & Kabocha, 2022).

In addition, the program for the avoidance of data loss is an effective instrument for the purpose of protecting a company's data. Data Loss Prevention (DLP) detects, monitors, and protects data while it is in use; data while it is in movement on the network; data while it is at rest in the data storeroom or on workstations, computers, mobile phones, or tablets; and data while it is at rest. DLP systems are responsible for the enforcement of data security rules. This is accomplished via in-depth content inspection as well as a contextual security analysis of transactions. They offer a centralized management system that can identify and stop the unlawful use of your personal information as well as prohibit its transfer. DLP safeguards against errors that may lead to data breaches and abuse on purpose by employees on the inside, in addition to protecting against assaults from the outside on corporate information infrastructure (Zhan et al., 2022).

3. Research Framework

This research makes use of a method called systematic literature review. It is an unbiased and objective research approach that aims to answer a set of research questions by conducting an analysis of all relevant literature in a particular subject area. In this research, the present state-of-the-art usage of security logs is identified, classified, and evaluated from a variety of points of view.

4. Future Research Agenda

This study is limited to identifying and preventing SQL injection attacks and makes use of a literature review. It is possible that in the future research will be carried out that is beyond the scope of the present study. This is especially true for small businesses that do not have the financial resources to strengthen their IT infrastructure to avoid assaults. In addition, strategies that seem to be more doable in such endeavors may be used to progress the study being conducted on the subject. In addition, the avoidance of data leakage may be a potential future line of study that might be generated from this research. Whereas, in this study, data security is attempted by the delivery of a key to the working agent, and without it the file cannot be shared, and the identification of a data leaker if any untrusted agent is engaged in harmful action. When the harmful behavior is attempted, the next item that will be crucial and essential will be the protection of sensitive data from leaking out. Agent information allocation on request via online mode is yet another feature that has room for improvement and expansion.

5. Conclusion

The research concludes that almost any authorized user who is in receipt of the data or information and can utilize his approved login credentials might potentially leak the data to third parties. The information about the leak is provided to the administrator or distributor of the database by the backend tracking SQL objects whenever he spills the data, whether he does it intentionally or not. These objects are included in the software's soft code, and they monitor the actions of the people who really are carrying out the work for the owner. This paper elaborates on and provides a summary of the attack idea as well as the attack implementation SQL injection attack Principles and Preventive Techniques for firms. The SQL injection process, as well as a demonstration of the SQL injection vulnerability exploitation approach by using manual SQL injection. The approaches that are discussed in this article may also be used for doing security testing on Web application systems that were written in other languages. This is since the attack concept has some degree of universality. Despite the ever-increasing sophistication of SQL injection technology, there will always be opportunities for exploits and threats to be concealed so long as programs and source code make use of the Internet.

6. References

2022 Data Breach Investigations Report. (2022). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Biswas, B., Mukhopadhyay, A., Bhattacharjee, S., Kumar, A., & Delen, D. (2022). A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums. *Decision Support Systems*, *152*, 113651.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*(5), e1211.

Papadimitriou, P., & Garcia-Molina, H. (2009, March). A model for data leakage detection. In *2009 IEEE 25th International Conference on Data Engineering* (pp. 1307-1310). IEEE.

Fang, Z., Xu, M., Xu, S., & Hu, T. (2021). A framework for predicting data breach risk: Leveraging dependence to cope with sparsity. *IEEE Transactions on Information Forensics and Security*, *16*, 2186-2201.

Fleury-Charles, A., Chowdhury, M. M., & Rifat, N. (2022, May). Data Breaches: Vulnerable Privacy. In *2022 IEEE International Conference on Electro Information Technology (eIT)* (pp. 538-543). IEEE.

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. *Journal of Financial Crime*.

Howard, P. N., & Gulyas, O. (2014). Data breaches in Europe: Reported breaches of compromised personal records in europe, 2005-2014. *Available at SSRN 2554352*.

Ghafarian, A. (2017, July). A hybrid method for detection and prevention of SQL injection attacks. In *2017 Computing Conference* (pp. 833-838). IEEE.

Gomez-Hidalgo, J. M., Martín-Abreu, J. M., Nieves, J., Santos, I., Brezo, F., & Bringas, P. G. (2010, August). Data leak prevention through named entity recognition. In *2010 IEEE Second International Conference on Social Computing* (pp. 1129-1134). IEEE.

Khoei, T. T., Slimane, H. O., & Kaabouch, N. (2022). A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions. *arXiv preprint arXiv:2207.07738*.

Liu, L., Han, M., Wang, Y., & Zhou, Y. (2018, June). Understanding data breach: A visualization aspect. In *International Conference on Wireless Algorithms, Systems, and Applications* (pp. 883-892). Springer, Cham.

Mills, J. L., & Harclerode, K. (2017). Privacy, mass intrusion, and the modern data breach. *Fla. L. Rev.*, *69*, 771.

Mukhopadhyay, I. (2022). Cyber threats landscape overview under the new normal. In *ICT Analysis and Applications* (pp. 729-736). Springer, Singapore.

Ping, C., Jinshuang, W., Lin, P., & Han, Y. (2016, October). Research and implementation of SQL injection prevention method based on ISR. In *2016 2nd IEEE International Conference on Computer and Communications (ICCC)* (pp. 1153-1156). IEEE.

Prabakar, M. A., KarthiKeyan, M., & Marimuthu, K. (2013, March). An efficient technique for preventing SQL injection attack using pattern matching algorithm. In *2013 IEEE international conference on emerging trends in computing, communication and nanotechnology (ICECCN)* (pp. 503-506). IEEE.

Qian, L., Zhu, Z., Hu, J., & Liu, S. (2015, January). Research of SQL injection attack and prevention technology. In *2015 International Conference on Estimation, Detection and Information Fusion (ICEDIF)* (pp. 303-306). IEEE.

Rode, M. K. N., Patil, M. A. R., Tare, M. S. V., & Kandane, M. S. S. (2020). Computer Network Security. *Journal homepage: www. ijrpr. com ISSN*, *2582*, 7421.

Saleem, H., & Naveed, M. (2020). SoK: Anatomy of Data Breaches. *Proc. Priv. Enhancing Technol.*, *2020*(4), 153-174.

Singh, N., Dayal, M., Raw, R. S., & Kumar, S. (2016, March). SQL injection: Types, methodology, attack queries and prevention. In *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 2872-2876). IEEE.

Sun, H., Xu, M., & Zhao, P. (2021). Modeling malicious hacking data breach risks. *North American Actuarial Journal*, *25*(4), 484-502.

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., ... & Bursztein, E. (2017, October). Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1421-1434).

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., ... & Bellekens, X. (2022). Cyber-security challenges in aviation industry: a review of current and future trends. *Information*, *13*(3), 146.

Voitovych, O. P., Yuvkovetskyi, O. S., & Kupershtein, L. M. (2016, September). SQL injection prevention system. In *2016 International Conference Radio Electronics & Info Communications (UkrMiCo)* (pp. 1-4). IEEE.

Verma, R., Gautam, V., Yadav, C. P., Gupta, I., & Singh, A. K. (2020, May). A Survey on Data Leakage Detection and Prevention. In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*.

Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2022). Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things*, 100544.

Yunus, M. A. M., Brohan, M. Z., Nawi, N. M., Surin, E. S. M., Najib, N. A. M., & Liang, C. W. (2018). Review of SQL injection: Problems and prevention. *JOIV: International Journal on Informatics Visualization*, *2*(3-2), 215-219.

Zhan, W., Yu, M., Jin, B., Guo, F., Deng, G., Liao, R., ... & He, X. (2022). Data Security Detection and Location Technology Based on DLP Network. In *International conference on Smart Technologies and Systems for Internet of Things* (pp. 469-477). Springer, Singapore.

Zuo, C., Lin, Z., & Zhang, Y. (2019, May). Why does your data leak? uncovering the data leakage in cloud from mobile apps. In *2019 IEEE Symposium on Security and Privacy (SP)* (pp. 1296-1310). IEEE.