**Database Security and Integrity**

Paul Farri

School of Business, Liberty University

CSIS-325 D02: Database Management Systems

Professor Tina Harclerode

April 26, 2022

**Abstract**

Database security and integrity are crucial aspects in the world of cyber security. When faced with the rising of threats such as SQL injection attacks, illegal access into databases by malicious individuals, tampering of important data, and shutdowns of government websites, it becomes all the more important in finding ways to curb these threats. Each of these types of attacks and beyond have the capability of severely damaging companies and harming many individuals. Companies however have tools that they can use to avoid the consequences of these attacks. Preventing unauthorized access, watermarking data, and maintaining data integrity by keeping the data unaltered, the likelihood of success in damages will be heavily limited. Hackers that steal from others demonstrate their intention of dishonoring God’s eighth commandment each time they steal, and the cyber security measures created act similar to how Christ shields the people of the world from sin. By extending the reach of the capabilities of cyber security and data integrity, computer systems and companies will be protected more so than they have ever been before.

**Database Security and Integrity**

**Introduction and Thesis Statement**

As technology evolves throughout the years, hackers and hostile organizations will take advantage of any potential opportunities to steal vital data from corporations, banks, and facilities that store their data in databases, using methods such as SQL injections, privilege abuse for illegal access, malware, and exploiting vulnerabilities. For every new generation of technology introduced, it becomes crucial to amplify the pursue of database security and integrity. Cyber security itself and database integrity are integral aspects of every computer and data system, as any type of computer and data system is vulnerable to at least some forms of breaches by cyber-terrorists, criminal organizations, malicious underground organizations, and data extortionists. Computer networks, data systems, and company servers may even be targeted by government spying agencies of countries from across the world, in which entire mainframes can be either hijacked or even shut down entirely. There is no computer system or database in the world that in invulnerable to cyber-attacks, as even the best possible protection has its own weaknesses and drawbacks (Jacyna et al, 2017) But with consistent action of cyber security tools, the likelihood of suffering from such crippling attacks can be lessened and even halted, keeping safe the precious and valuable data that companies rely on.

**Database Security and Integrity**

**Problem Statement**

In today’s technological environments, hackers are successfully advancing in various ways of infiltrating databases to steal important information and data from companies and government entities. Some of the most targeted data systems by hackers are databases, as they face the highest rate of breaches compared to other business assets in a company. Verizon’s Data Breach Report in 2012 states 96% of the total records that are breached come from databases. According to Open Security Foundation, in the year 2012 alone, as many as 242.6 million records of data were potentially compromised by hackers (Singh & Rai, 2014).

Some ways that hackers and malicious users can access database records is through excessive privilege abuse, SQL injections that can take down websites, and taking advantage of system vulnerabilities. For example, excessive privilege abuse is when access privileges for the database are in the hands of abusive applications or malicious end users that try to exceed their job function requirements, bypassing set limitations. This form of security breach can happen because sometimes database administrators might lack the time or opportunity to update and configure the access control mechanisms for each individual end user, resulting in some end users having more to access than what is necessary. An example of this is with a university professor. This professor who only has the authority to change student contact information may attempt to change the student’s grades at the same time which goes beyond his job function. A good way to prevent this abuse is by enforcing query-level access control. This allows for database privileges to be restricted and makes the end user to only be able to use simple, minimum-required SQL operations such as UPDATE and SELECT. If the professor attempted to change the student grades while under query-level access control, an alert would be sent out (Singh & Rai, 2014).

The implications of a Biblical worldview in this issue of cyber security and data integrity are revealed based upon the hacker’s lack of honoring God’s commandment regarding coveting and stealing. Christ has always taught and made clear to His creations that to steal from your neighbor goes against God’s law. Thief of someone’s property and the breaking of the eighth commandment, “Thou Shall Not Steal”, is a violation of that sacred word that He has inscribed unto his creations. When a hacker steals from a company or an individual, they are expressing their decision to dishonor God.

**Purpose Statement**

Cyber security must be expanded in the field of databases. This means enforcing further measures in implementing proper access privileges to employees, cracking down on worms and injections sent by hackers, and maintaining consistent database integrity. Without these measures enforced, databases will become far more vulnerable. Small measures may be able to hold back a few hacking individuals, but stricter measures are needed if companies wish to be protected from larger and more capable entities, such as cyber terrorist groups. Data integrity must also be strictly maintained, as doing so can aid in keeping databases both secured and well-organized.

The goal of this research paper’s examination of this topic is to inform of the dangers of hackers and give light to the importance of cyber security for databases, and to help solve the problem in overcoming hackers and data-pirates. Technology is such a widely adopted aspect of human engineering and innovation, and most countries across the world utilize it in some way, shape, or form. This technology opens many doors, many of which are both good and bad.

**Database Security and Integrity**

**Literature Review**

Examples of how hackers have affected countless facilities in the past can be seen very easily. Online healthcare databases are usually a frequent target for cyber criminals and hackers because they contain the records of many people who have visited the facility. This allows for them to be able to conduct identity theft by stealing the records and using their information to steal even more of their assets (Kaddoura et al, 2021). When databases are at risk by hackers or from a breach in security, they typically take place in the interfaces connected to the database, the database’s server, the database management system along with its interface, and even the computer’s operating system (Jacyna et al, 2017).

Many nations’ government websites around the world each year are also heavily affected by a form of security breach called SQL injection attacks. SQL injection attacks use coding techniques that trick the database application into giving illegal access to malicious end users. These types of cyber-attacks typically target websites 65% of government websites for developing countries are vulnerable to SQL injections. This makes websites vulnerable to getting shut down entirely, or even having very important information stolen (Dorai et al, 2011). Data integrity in databases is also important to have, as doing so can protect a database and maintain data organization. One way this can be done is to prevent unauthorized access and unauthorized changes from individuals without legal access. Through the implementation of the universal basis of relations, this will make sure that the data within the database is unmodified, unaltered, and undistorted (Yesin et al, 2021). Another way to maintain data integrity and data security is by digital watermarking. This allows for data to remain uncompromised and maintain complete integrity and value, even if it is stolen by a hacker or cybercriminal. Reversible watermarking can also allow for any lost or degraded data to be restored during a situation in which the data is stolen, which can be very useful for hospitals (Tufail et al, 2019). As a whole when it comes to database security, some of the best ways overall in figuring out solutions to counter these cyber threats are learning from mistakes and analyzing from past scenarios (Blake, 2007).

**Database Security and Integrity**

**Implications of the research paper**

This research paper is relevant to the Biblical worldview in accordance with Exodus 20:15-17, in which God commands his followers that they shall not steal nor covet their neighbor’s property (King James Bible 1769/2017, Exodus 20:15-17). According to Ephesians 4:28, a thief should no longer steal from his neighbor, but instead be encouraged to conduct labor, in which he should do honest work from his own hands and share what he makes to those who need it (King James Bible 1769/2017, Ephesians 4:28). Cyber criminals that have been reformed from the world of crime are now using their skills to help others and share with what they know, such as working with law enforcement to catch other cyber criminals so that they may be brought to justice. This fulfills what Christ meant in terms of a thief turning from greed and wickedness and pursuing honest work to produce fruit that may be shared with others.

The topic this research paper examines is relevant to industries and managers based on the cases that hackers can make companies lose millions of dollars a year for every amount of data that may be stolen, as well as vital corporate information that may be used for blackmail and extortion. If a company is brought to its knees, then every person working in the company will suffer for it. Jobs would very likely be lost at the same time, resulting in workers losing their financial sustainability. And if one major company falls, another one is likely to follow unless the threat is eliminated or kept at bay until a solution is found.

**Database Security and Integrity**

**Biblical worldview implications**

Just as many other aspects of human life, human actions, and other worldly things have their own biblical implications, cyber security is no different. Cyber security in a way is similar to how God protects His people from the chains of evil and the dangerous grips of sin. His Holy Bible is the ultimate firewall for humans, and His disciples are the sources of protection that root out the viruses, malware, and SQL injections within our lives.

If companies across the world have the access to data from people, it allows them to set up adjustments to help improve the company’s products, policies, or ability to forecast shifts in business. While sending valuable customer data to a company will always carry risks, such data can be very helpful for companies seeking to improve themselves and their businesses. It is important for customers to be aware of the risk, and to be able for a sense of trust with the company if the company is able to prove that it won’t use the data for malicious purposes.

When personal data is handed to a company or service, it becomes their responsibility to make sure that the data remains in a safe environment, just as how Biblical figures entrusted others to watch over their property in their absence. Personal data within a database is considered a person’s property, regardless of the hands that it falls into. Stealing this personal data falls under the Biblical implication of stealing a neighbor’s property, because the information came from the owner’s hands or as a result of fruits from their labor.

**Conclusion**

Each advancing generation of technology open newfound windows for hackers to find ways to advance their own skills and abilities to infiltrate databases and overcome older security measures. That is why the security measures themselves as well as the drive to enforce cyber security in databases must be just as advancing and pursued for the sake of protecting nationwide systems. Without the necessary measures put into place and conducted when needed, vital data will become lost, and such a loss can potentially bring any company or government to their knees. But when those necessary measures are in place, hackers and cyber criminals lose morale and the motivation to target protected systems.

**References**

Blake, E. A. (2007). Network and database security: regulatory compliance, network, and database security - a unified process and goal.*The Journal of Digital Forensics, Security and Law : JDFSL, 2*(4), 77-106.

Dorai, R., & Kannan, V. (2011). SQL injection-database attack revolution and prevention.*Journal of International Commercial Law and Technology, 6*(4), 224.

Jacyna, M., Gołębiowski, P., Szczepański, E., & Wasiak, M. (2017). *Efficacy of data security in managing the database of SIMMAG 3D system*. Vilnius Gediminas Technical University, Department of Construction Economics & Property. http://dx.doi.org.ezproxy.liberty.edu/10.1016/j.proeng.2017.04.410

Kaddoura, S., Haraty, R. A., Kontar, K. A., & Alfandi, O. (2021). A parallelized database damage assessment approach after cyberattack for healthcare systems.*Future Internet, 13*(4), 90. <https://doi.org/10.3390/fi13040090>

*King James Bible.* (2017). King James Bible Online. <https://kingjamesbibleonline.org/> (Original work published 1769)

Singh, S., & Rai, R. K. (2014). A review report on security threats on database. *International Journal of Computer Science and Information Technologies*, *5*(3), 3215-3219.

Tufail, H., Zafar, K., & Baig, A. R. (2019). Relational database security using digital watermarking and evolutionary techniques.*Computational Intelligence, 35*(4), 693-716. <https://doi.org/10.1111/coin.12209>

Yesin, V., Karpinski, M., Yesina, M., Vilihura, V., & Warwas, K. (2021). Ensuring data integrity in databases with the universal basis of relations.*Applied Sciences, 11*(18), 8781. <http://dx.doi.org.ezproxy.liberty.edu/10.3390/app11188781>