Displaying StreamList User Events: Part 2

Pantea Namiranian

The University of Arizona Global Campus

INT499: Capstone for Information Technology (INP2520A)

John Russell

5/26/2025

Displaying StreamList User Events

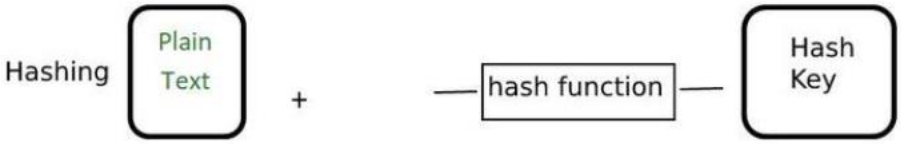
As we know in today's online world, protecting user information and data security is critical. Passwords are often the first line of defense against unauthorized access to sensitive data. Here we will summarize the first two stages of password protection, explain the purpose of hashing in authentication, and discuss how hashing is different from encryption. This paper will also cover the limitations of hashing, compare storing passwords in cleartext versus using hashing, and explain why hashing is a secure way to store passwords. Finally, it will look at the ethical, legal, and security concerns that can arise from these practices. The goal of this paper is to highlight the importance of strong password protection methods to keep user data safe.

Stages of Password Protection

The first two stages of password protection are password creation and storage. In the password creation stage, users should make strong passwords that are hard to guess. This means using a mix of uppercase and lowercase letters, numbers, and special characters while the second stage focuses on securely storing these passwords. This is where hashing comes in, which converts the original password into a fixed-length string of characters, making it unreadable and protecting it from unauthorized access. "In the 1970s a famous researcher Robert Morris Sr. has adapted the method called "hashing" to password security. A hash function is designed to map data of random sizes to a fixed-size data. In cybersecurity, this function is also devised to be a one-way (sometimes called a "trapdoor") function—easily computable, but infeasible to invert or backtrack. This cryptographic hash function takes user input—the password—and turns it into a seemingly random sequence of numbers" (PassCamp).

Purpose of Hashing in Authentication

As we have mentioned above hashing is used in authentication to turn a password into a unique hash value. Instead of storing the actual password, the hash value is saved. When a user tries to log in, the password they enter is hashed again, and the new hash is compared to the stored hash. If they match, access is granted. This method ensures that even if the database is hacked, the actual passwords remain secure. “Generally, the hash keys are stored in the database, and they are compared to check whether the original information matches or not. They are generally used to store the passwords for login. Some of the examples of a hashing algorithm are MD5, SHA256” (geeksforgeeks).



Hashing vs. Encryption

Hashing is different from encryption because hashing is a one-way process, while encryption can be reversed. Hashing takes an input (the password) and produces a fixed-size string that cannot be changed back to the original input. On the other hand, encryption transforms data in a way that it can be reversed with a decryption key. This difference makes hashing a better choice for password storage since it ensures passwords cannot be retrieved even if the hash is known. As Dinu Gitlan explains in Medium “Encryption transforms data using a key, making it unreadable to unauthorized users. It’s reversible with the right key. Hashing generates a fixed-size hash from input data, providing a unique fingerprint. It’s one-way and not reversible. Encoding converts data for compatibility but is easily reversible, serving formatting purposes, not security” (Gitlan. D, 2024).

Limitations of Hashing

Despite its benefits, hashing has limitations. One major issue is that if two users have the same password, they will produce the same hash, making it easier for attackers to crack passwords using precomputed tables (known as rainbow tables). Additionally, if a hashing algorithm has weaknesses, all passwords hashed with that method may be at risk.

Cleartext vs. Hashing Mechanisms

Storing passwords in cleartext is very risky. If a database is compromised, attackers can easily access all user passwords. In contrast, using hashing mechanisms adds security because the original passwords are not stored. This difference highlights why hashing is necessary for protecting user data. As Christophe said “The purpose of encryption is to secure the confidentiality of data, while the purpose of hashing is to protect the integrity of the information. Another difference is that hashing will generate a fixed-length value once the data is passed through a hashing function, whereas encryption will generate different length data” (Christophe, 2022).

Concept of Hashing in Password Storage

Hashing in password storage means converting passwords into hash values using a hashing algorithm. This process works by applying a mathematical function to the password, creating a unique hash that represents the original input. Hashing is considered a more secure approach because it makes it nearly impossible to retrieve the original password from the hash. Even if someone gains access to the hash, they cannot easily figure out the password. “Hashing is widely used for secure password storage. Instead of storing passwords in plain text, they're hashed and stored as hash values. This adds an extra layer of security so even if the hash values

are compromised, it's computationally infeasible to reverse-engineer the original passwords" (TechTarget).

Ethical, Legal, and Security Concerns

The first two stages of password protection raise ethical, legal, and security concerns. Ethically, developers must implement strong password protection measures to keep user data safe. Legally, organizations could face serious consequences if they do not protect sensitive information properly. Security concerns arise from the possibility of data breaches, which can lead to identity theft and loss of trust from users.

Conclusion

In conclusion, effective password protection is crucial for keeping user data safe in today's digital world. Hashing plays an important role in this process by providing a secure way to store passwords. Understanding the differences between hashing and encryption, as well as the limitations of hashing, is vital for developers and organizations. By following strong password protection practices, we can improve user security and build trust in online platforms.

GitHub Repository

For the complete code of the StreamList application, please visit my GitHub repository: [https://github.com/panteanam/Pantea-Namiranian-INT499-Week-2-Assignment-Part-1.git].

References:

(Sep 2018). *4 levels of password security.* https://passcamp.com/blog/4-levels-of-password-security/

Gitlan, D. (Feb 2024). *Encryption vs Hashing: What's the Difference?* https://medium.com/

Difference between Hashing and Encryption. https://www.geeksforgeeks.org/difference-between-hashing-and-encryption/

Christophe. (June 2022). *Encrypted versus hashed passwords. What's the difference?* https://cybr.com/certifications-archives/encrypted-versus-hashed

Yasar, K. (May2024). *Definition Hashing.* https://www.techtarget.com/searchdatamanagement/definition.

Wargo, J. M. (2020). Learning Progressive Web Apps. Pearson Technology Group.