IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBER SECURITY - PASSWORD STORAGE IN BROWSER

Prof. Mayur Chavan
Prof. at SCTR's Pune Institute of Computer Technology.

Akshay Lahoti
Student at Computer Engg. Dept. SCTR's Pune Institute of Computer Technology.

Ayush Meshram
Student at Computer Engg. Dept. SCTR's Pune Institute of Computer Technology.

Aditya Londhe
Student at Computer Engg. Dept. SCTR's Pune Institute of Computer Technology.

Abstract - In the era of digital connectivity, securing online accounts has become a top priority. The surge in the number of online accounts managed by an individual has led to an increase in the number of passwords that need to be remembered and managed. Moreover, the growing sophistication of cyber attacks has highlighted the need for more advanced and robust security measures. Our proposed solution is a browser extension model designed to tackle these challenges by offering a secure and user-friendly solution for password management. The model integrates several key features aimed at enhancing both security and usability. The extension provides a centralized repository for storing passwords for multiple online accounts, eliminating the need for users to remember multiple passwords and reducing the risk of password loss or theft. To protect sensitive user passwords, the extension uses the robust encryption algorithm, a cryptographic technique known for its strength and resistance to unauthorized decryption attempts. Unlike many other password management solutions that store data on the cloud, our extension stores passwords locally on the user's device. This approach enhances data privacy and reduces the risk of exposure to external threats. The extension also allows users to decrypt their stored passwords as needed, ensuring that users have access to their passwords when required, without compromising security. The extension is designed with a user-friendly interface that simplifies storing, managing, and retrieving passwords. It also includes features such as auto-fill and one-click login for added convenience. By integrating these features, our browser extension model offers a practical and secure solution for managing digital identities. It marks a significant advancement in addressing the challenges associated with password management in today's digital era. Our proposed browser extension model provides a comprehensive solution to the pressing issue of secure password management in the digital age. By integrating robust security features with user-friendly design elements, we aim to provide users with a tool that not only enhances their online security but also simplifies their digital lives.

Keywords - Data Privacy, Browser Extension, Password Management, Password Storage, Encryption, Local Device Storage, Data Security, Password Security, Digital Identity, Online Accounts, Cryptographic Techniques, Decryption, Cybersecurity, User Convenience, Password Access, Password Encryption, Online Security, Browser Security.

I. INTRODUCTION

Cybersecurity is the comprehensive practice of protecting computer systems, networks, and sensitive data from a multitude of potential threats that could lead to unauthorized access, theft, or damage. In today's digital environment, it has

evolved into a critical issue that impacts individuals, businesses, and governments. Cyber threats come in many forms, including malware (such as viruses, worms, trojans, and ransomware), phishing attacks (deceptive emails and websites designed to trick users into divulging confidential information), denial of service attacks (DoS) (overwhelming systems to compromise their availability), social engineering tactics (manipulating individuals to reveal sensitive data), data breaches (unauthorized access to confidential information), and insider threats (malicious or negligent actions by employees or trusted entities). Cybersecurity relies on a variety of security measures and technologies to mitigate these threats. Firewalls act as protective barriers, filtering incoming and outgoing network traffic to prevent unauthorized access. Antivirus software is designed to detect and remove malware, and intrusion detection systems (IDS) and intrusion prevention systems (IPS) continuously monitor network traffic for suspicious activity and can take steps to block potential threats. Encryption plays a key role in protecting data by converting it into a secure format that can only be decrypted with the appropriate decryption key. Multi-factor authentication (MFA) increases security by requiring users to provide two or more forms of identification before being granted access to systems or accounts. Regular patch management keeps software and systems up-to-date with the latest security patches and prevents vulnerabilities from being exploited. Additionally, implementing robust security policies and providing user training are essential components of a robust cybersecurity strategy. Saving passwords in web browsers is a practice that offers both convenience and potential cybersecurity risks. The primary benefit lies in the sheer convenience it provides to users by simplifying the login process. This feature allows users to save their login information for different websites, eliminating the need to remember or manually enter passwords each time they visit. Additionally, many modern web browsers include built-in password generators that encourage the use of complex and strong passwords, which is essential for overall cyber security. Cross-device synchronization further improves the user experience by enabling seamless access to saved passwords across platforms. However, this convenience is not without its vulnerabilities. Security concerns arise, especially when unauthorized access occurs to a user's device or browser. Without a master password, some browsers pose security risks because they allow anyone with physical access to view and use saved passwords. Additionally, automating password entry can make users more susceptible to phishing attacks, where fake websites impersonate legitimate ones, which can lead to unauthorized account access. Additionally, browsers generally lack the advanced security features present in dedicated password managers. These specialized tools often offer stronger encryption, two-factor authentication, secure password sharing, and password strength analysis.

To mitigate these risks, users are encouraged to use a master password when available, keep browsers updated, generate strong unique passwords, be careful when clicking on links, and consider dedicated password managers for added security. By adopting these best practices, users can balance convenience with cybersecurity concerns and make an informed decision whether to use an in-browser password store or opt for a dedicated password manager that suits their individual needs and preferences.

II. CRYPTOGRAPHY

Cryptography is the technique of securing information and communications through the use of codes, so that only those for whom the information is intended can understand and process it. It prevents unauthorized access to information. The techniques used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms. There are several types of cryptographic algorithms available. They vary in complexity and security, depending on the type of communication and the sensitivity of the information being shared. Some of the most common types include:

1] Symmetric Key Cryptography: An encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages.

2] Hash Functions: There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered.

3] Asymmetric Key Cryptography: Under this system, a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption.

The analysis of cryptography involves studying these algorithms for their effectiveness in securing data, their resistance to various attacks, and their efficiency in terms of computational resources. It also involves analyzing protocols that prevent malicious third parties from retrieving information being shared between two entities. This analysis helps in ensuring data confidentiality, integrity, authentication, and non-repudiation.

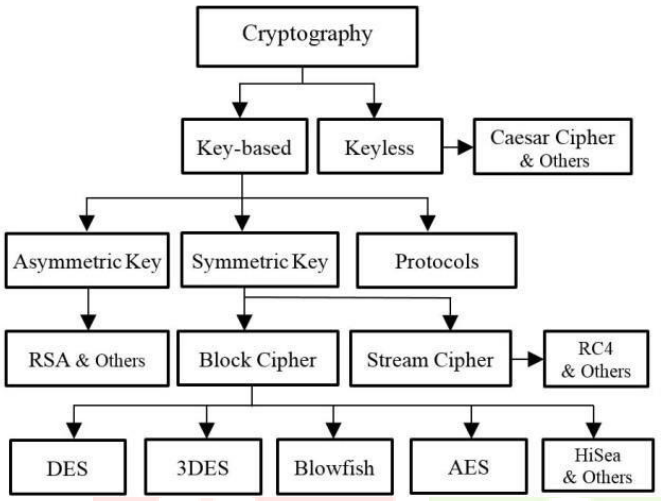

Fig 1. Types of Cryptography

Cryptography is a vast field with numerous applications in the digital world. Here are some additional aspects of cryptography:

1] Digital Signatures: Digital signatures are a cryptographic technique often used to verify the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender and that it was not altered in transit.

2] Cryptanalysis: Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. It is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

3] Cryptographic Protocols: They are widely used for secure application-level data transport. A cryptographic protocol usually involves multiple parties and includes steps involving computations or operations to be performed on input data to achieve a desired result.

4] Quantum Cryptography: Quantum cryptography is an attempt to allow two users to communicate using more secure methods than those guaranteed by traditional cryptography. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication.

Remember, while cryptography is essential for secure communications, it's equally important to keep your cryptographic systems up-to-date. As computational power increases, cryptographic algorithms can become vulnerable and may need to be replaced with more robust or complex algorithms. Hashing and encryption are two terms used widely in cryptography. Encryption is the process of converting a normal readable message known as plaintext into a garbage message or not readable message known as ciphertext. The ciphertext obtained from the encryption can easily be transformed into plaintext using the encryption key. Some of the examples of encryption algorithms are RSA, AES, and Blowfish. On the other hand, hashing is the process of converting the information into a key using a hash function. The original information cannot be retrieved from the hash key by any means. They are generally used to store the passwords for login. Some of the examples of a hashing algorithm are MD5, SHA256.

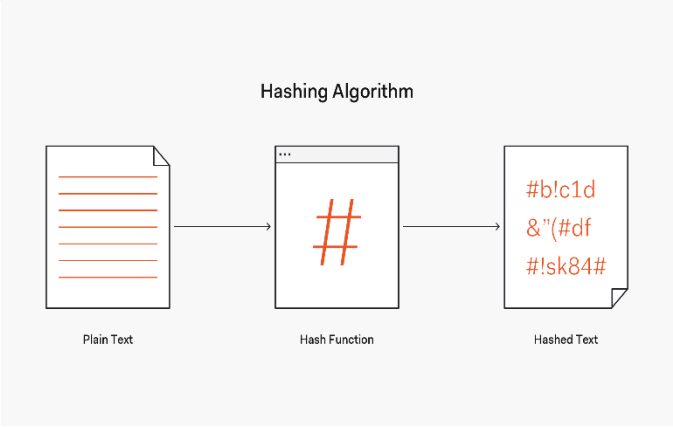

Fig 2. Working of Hashing Algorithm

III. Encryption Algorithms

1] Triple DES: Triple DES is a block cipher algorithm that was created to replace its older version, the Data Encryption Standard (DES). It has a key length of 168 bits (three 56-bit DES keys), but due to meet-in-middle-attack, the effective security is provided for only 112 bits2.

2] RSA: RSA is an asymmetric key algorithm named after its creators Rivest, Shamir, and Adleman. The algorithm is based on the fact that the factors of large composite numbers are difficult to find when the integers are prime2.

3] Twofish: Twofish algorithm is the successor of the Blowfish algorithm. It uses a single key of length 256 bits and is said to be efficient both for software that runs in smaller processors such as those in smart cards and for embedding in hardware2.

4] AES (Advanced Encryption Standard): AES is a symmetric block cipher chosen by the United States government to protect significant information. AES has three 128-bit fixed block ciphers of keys having sizes 128, 192, and 256 bits2.

5] Blowfish: Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits1.

6] IDEA (International Data Encryption Algorithm): IDEA is a symmetric key block cipher developed by James Massey of ETH Zurich and Xuejia Lai and was first described in 1991. It was intended as a replacement for the Data Encryption Standard1.

7] ECC (Elliptic Curve Cryptography): ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields2.

IV. Various Hashing Algorithms

1] MD5 (Message Digest Algorithm 5): MD5 is fast and produces a 128-bit (16-byte) hash value. However, it is considered cryptographically broken and unsuitable for further use due to vulnerabilities like collision attacks. It's not recommended for security-critical applications. MD5 (“hello world”) = fc5e038d38a57032085441e7fe7010b0

2] SHA-1 (Secure Hash Algorithm 1): SHA-1 produces a 160-bit (20-byte) hash value and is faster than more secure alternatives. However, SHA-1 is no longer considered secure for cryptographic purposes because of vulnerabilities to collision attacks. It is also not recommended for secure applications. SHA-1 (“hello world”) = 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed

3] SHA-256 and SHA-3: These are part of the SHA-2 and SHA-3 families, respectively, and produce longer hash values (256 bits or more), making them more secure. They are widely used in various security applications. SHA-256 (“hello world”) = b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

4] bcrypt: bcrypt is specifically designed for securely hashing passwords. It incorporates a salt to protect against rainbow table attacks. It is computationally intensive, which can be a limitation in high-traffic applications, but it's a necessary trade-off for password security. Bcrypt (“hello world”) = $2a$12$DvjTT3zR3i85.PVVFvn2VuCt0M8s9T/cM22B1tiZBIUxsPStQ.6Ga (Note: bcrypt hashes will vary because of the salt)

5] Scrypt: Similar to bcrypt, scrypt is designed for secure password hashing and adds memory-hardness to resist brute-force attacks. It's even more computationally intensive than bcrypt, which can be a limitation in resource-constrained environments. Scrypt (“hello world”) =702edca0b2181c15d457eacac39de39fc8497a2e9b0ae2c8e7ef7487a6ba1aae (Note: Scrypt hashes will vary because of the salt)

6] HMAC (Hash-based Message Authentication Code): HMAC is used for data integrity and authenticity verification, making it a reliable choice for this purpose. HMAC (using SHA-256) (“hello world”) = 87aa7a5354316b143ad57b390fd9a3dfb8a1b16f35a7b4c24423825c8fd62164

7] MurmurHash: MurmurHash is a non-cryptographic hash function known for its speed and simplicity. It's often used for tasks like hash tables and data structures. MurmurHash(“hello world”) (32-bit) = df5f619040

8] CRC32 (Cyclic Redundancy Check): CRC32 is a fast checksum used for error detection in network communications and data storage. CRC32(“hello world”) = 0d4a1185

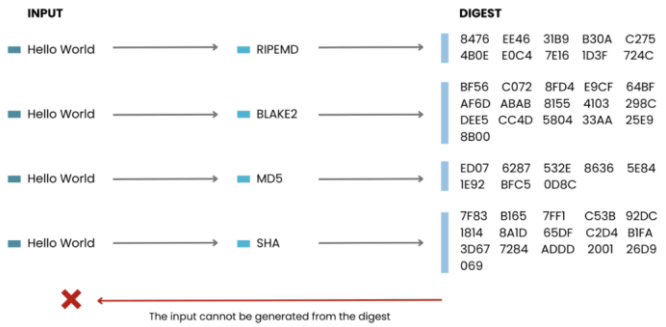

Fig 3. Examples of Some Hashing Algorithms

V. COMPARISON BETWEEN ENCRYPTION AND HASHING

Hashing and encryption are two fundamental cryptographic techniques that play different roles in data security, and a detailed comparison will reveal their fundamental differences and specific applications.

Hashing is a one-way function that takes an input (data in plain text format) and produces a fixed-length string of characters known as a hash value or digest. It is primarily used for verifying data integrity, securely storing passwords, and creating data structures such as hash tables. Hashing is irreversible, meaning it is virtually impossible to reverse the process and get the original input from the hash value. Additionally, the same input will consistently produce the same hash value, ensuring determinism.

One of the key applications of hashing is the secure storage of passwords. When a user creates an account or sets a password, the system stores the password hash rather than the password itself in plain text. During authentication, the system hashes the entered password and compares it with the stored hash. If they match, the password is considered valid. Since the original password cannot be derived from the hash, this method increases security, especially in the event of a data breach.

Hashing is also used for data authentication. When transferring files or data, hash values can be calculated before and after the transfer, and if the hash values match, it means that the data was not tampered with during the transfer. This is commonly used with checksums and digital signatures.

Encryption, on the other hand, is a reversible process that uses an encryption key to transform plaintext data into ciphertext. It is primarily used to protect data confidentiality and ensure that unauthorized users cannot access the original data. Encryption is commonly used in scenarios where data needs to be securely transmitted or stored. There are two main types of encryption:

1. Symmetric Encryption: In this method, the same key is used for both encryption and decryption. It is effective for bulk data encryption, but requires secure key distribution to maintain confidentiality.
2. Asymmetric encryption: Asymmetric encryption uses a key pair, a public key for encryption and a private key for decryption. The security benefits are that the private key never leaves the owner's control and the public key can be freely shared. It is often used for secure communication and digital signatures.

Encryption is used in scenarios such as secure communication over the Internet (eg HTTPS for web traffic), secure file storage, and protection of sensitive data in databases. When data is encrypted, it can only be decrypted using the appropriate decryption key, making it a powerful tool for maintaining data confidentiality.

In short, while both hashing and encryption are cryptographic techniques, they serve different purposes and have unique properties. Hashing is a one-way, irreversible process used primarily to verify data integrity and securely store passwords. Encryption is a reversible process that focuses on data confidentiality and ensures that data is protected from unauthorized access. Each technique has its own set of use cases, and their selection depends on the specific security goals and requirements of the task at hand.

CONCLUSION

In conclusion, the proposed browser extension model stands as a beacon of innovation in the realm of digital security. It addresses the pressing need for robust password management, offering a secure and user-friendly solution that integrates advanced encryption techniques with a user-centric design. By storing passwords locally and providing features such as auto-fill and one-click login, it not only enhances online security but also simplifies the user experience. This model represents a significant step forward in our digital age, providing a comprehensive solution to the challenges of

password management and setting a new standard for digital identity protection. It is our hope that this tool will empower users to navigate their digital lives with greater confidence and ease, knowing that their online identities are securely managed.

FUTURE WORK

Future work on storing passwords in web browsers, using hashing and encryption algorithms, holds the promise of addressing both evolving security issues and user expectations. As cyber threats continue to proliferate, one potential improvement is the development of adaptive and resilient password hashing techniques. This may include integrating memory-intensive features and strategies to effectively counter emerging attack vectors. In addition, post-quantum cryptography could play a key role in securing password encryption as quantum computing capabilities develop, making it imperative to explore quantum-resistant encryption schemes. In addition to these technical improvements, future work should also prioritize improving the user experience by simplifying password management, potentially incorporating biometric authentication, and supporting strong authentication procedures.

In addition to technical progress, interoperability and standardization efforts are essential. Researchers should focus on developing cross-browser solutions that facilitate secure and seamless password management. Additionally, decentralized and user-centric identity solutions such as self-sovereign identity (SSI) and blockchain-based authentication represent a transformative direction for the field. These technologies offer users more control over their credentials and data, reducing reliance on traditional passwords. In short, the future of browser-based password storage involves a multifaceted approach that includes cutting-edge cryptographic techniques, user-friendly interfaces, security measures that adapt to the evolving threat landscape, and innovative identity solutions that together contribute to a more secure user-centric digital ecosystem.

ACKNOWLEDGMENT

We express our sincere appreciation to Prof. M. S. Chavan, our STC guide, whose expertise and guidance significantly contributed to our research's success. His valuable insights, unwavering support, and commitment to excellence played a crucial role in shaping the trajectory of our work.

REFERENCES

[1] Vadhera Priyanka, "BhumikaLal – Review Paper on Secure Hashing Algorithm and Its Variants", ISSN (Online): 2319-7064 International Journal of Science and Research (IJSR), pp. 629-632, 2012.

[2] Bart PRENEEL - Analysis and Design of Cryptographic Hash Functions, pp. 1-30, February 2003.

[3] N. Jirwan, A. Singh and S. Vijay, "Review and Analysis of Cryptography Techniques", International Journal of Scientific & Engineering Research, vol. 3, no. 4, pp. 1-6, 2013.

[4] A. Gupta and N. K. Walia, "Cryptography Algorithms: A Review", INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, vol. 2, no. 2, pp. 1667-1672, 2014.

[5] Rohit, S. Kamra, M. Sharma and A. Leekha, "Secure Hashing Algorithms and Their Comparison," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2019, pp. 788-792.

[6] Extensions - Chrome for Developers https://developer.chrome.com/docs/extensions/