**Reducing risks of data theft: Hashing vs. Asymmetric encryption**

**Research Methods**

**Student Name** : **Sagarika Nagaraj**

**Student ID** : **17061633**

# 

# Abstract

The bases of the research are focused in the domains of maintaining different practices established in the measure of providing considerations in case of providing protection. This measure of protection is the consideration which is developed in the bases of aligned infrastructure and the mechanisms of hashing and asymmetric course of interactions are to be weighed. These alignments provide knowledge which is necessary in the build of provisions which are to be on the track of appropriate notion of functioning establishments. The Password-Based Key Derivation Functions (PBKDF) is carried out in the course of alignment of the functions through which the passwords are converted into secret keys. This process tends to maintain the fixed size cipher function of operation in direction for the keys. The PBKDF is also called Hashing. The measure of Asymmetrical cryptography also provides the bases of antitheft measures. This paper involves the methodology which has been utilized in order to complete the research. There are multiple areas on which the discussion been done in the paper. Making effective papers required a strong knowledge of the methodology. The methodology is one the prime factor which helps the particular complete the research.

Table of Contents

[Abstract 2](#_Toc46767486)

[Introduction 4](#_Toc46767487)

[Research Question 5](#_Toc46767488)

[Aims and Objectives 5](#_Toc46767489)

[Background 5](#_Toc46767490)

[Methodology 6](#_Toc46767491)

[Research Design 6](#_Toc46767492)

[Research Approach 7](#_Toc46767493)

[Result 9](#_Toc46767494)

[Discussion 9](#_Toc46767495)

[Reference 11](#_Toc46767496)

# Introduction

Different programs are used in the course of software programming to depict the bases of encrypted security of the user information. These are the programs in which the passwords are protected with the course of evaluation in which the public key cryptology is maintained to sustain the usability of password protection through the appropriate protection provisions from the bases of unauthorized access are maintained. These are the infirmities of the information which is entitled to the initiator of the key alone (Sapkota, 2015). In the same manner, there are procedures of different bases which are carried out in the assessment of hashing of the passwords by the implication of procedure to convert them into bases are visible to the initiator and provides the stance of protection against unauthorized access. These are the procedures that are expanded through the content analysis and the bases of studying preceding literature. Hashing is one of the most important and secure technique to secure passwords. There are multiple tools and techniques which can make the password more secure, but on the other hand, hashing is somehow more different, and the other advantage of hashing is that the hackers cannot reverse the code. This makes the password more strong and efficient. Hashing is a programming technique that is utilized to make the passwords of the computer stronger, so there is less chance for antitheft. The strength of the hashing explains the policy regarding the password for the user(Raymond, 2017).

# Research Question

Can the measure of data theft be reduced by the implications of hashing and asymmetrical encryption?

# Aims and Objectives

The research is focused on the bases of the following aims and objectives:

* The assessment of the different protection measures for data from theft.
* Analyses of data protection through hashing.
* Evaluation of data protection through asymmetrical encryption.

# Background

The build of background is developed in such a measure that the assessment of the different executions of protection is evaluated from the propensities of maintaining antitheft. The establishment of grounds on the bases of security establishment carried out the course of aligned procedures that are necessary for the protection grounds (Toapanta, Astudillo, & Gallegos, 2020). The opted methodology is an unfocussed summary that is evaluated in the course of assessing and analyzing the basis which is sustained as per the developmental analysis and the distinctions of the behavior of the discipline. These are the stance of the methodological bases, which will provide the depiction of analysis through the maintenance of procedures that are necessary to sustain the course of database safety and protection.

The world has advanced, and technology is evolving so fast. As the innovations are introduced for better use and protection of data, new risks and threats are also coming into the market. Cybercrime and data theft have increased to a great extent, and companies are facing big threats from hackers and other criminals. In past years, many bank accounts were hacked, and banks lost a lot of people’s money. Hacking of ATM passwords has become common nowadays, and people are losing their money and assets. New cybersecurity and programming techniques are introduced and applied by the banks and other organizations to stop the theft of confidential data.

Cyber algorithms are developed to stop the data-stealing by encrypting and decrypting the data. The data and password become difficult to hack, and thus companies get data protection and integrity. Symmetric and Asymmetric encryption is used to encrypt and decrypt the data by scrambling all the useful data to make it difficult for the hacker to access the required data patches. Hashing is the most commonly used technique to incorporate companies because it provides greater data authentication and integrity. Hashing makes the different string indexes for each of the data values, and that data cannot be reversed back to its original value.

Companies are using hashing and asymmetric techniques more because their cryptography techniques are more reliable. Data is scrambled into different locations and indexes, and hackers fail to decrypt that data. In this modern world, all the financial and operational data is stored digitally and can be used illegally by just entering into the server. Many state and federal agencies are involved in the cybercrime and trying their best to stop this crime. The government is paying more to the tech companies to upgrade these techniques for better control of data protection and circulation.

**Literature Review**

[Rafael Alvarez](https://sciprofiles.com/profile/245297) and his fellow partners researched in 2018 on optimizing the hashing function with symmetric encryption for passwords (Álvarez, Andrade, & Zamora, 2018). The study was focused on the functions used in symmetric keys for better password hashing so that no one could hack the password. The researchers used qualitative research and gathered information from previous studies. From results, they proposed that cybersecurity could be achieved by applying AES as a pseudorandom generator and taking benefit of hardware acceleration for AES. The researchers analyzed the characteristics of hashing and symmetric cryptography and compared them with other algorithms like Argon2 and Scrypt for the better application of research findings.

In 2016, research was done by Fatma Omara and her partners on the hybrid hashing security algorithm for data storage on cloud technology (Omara & AbdElnapi, 2016). Cloud technology is the fastest growing technology in the modern era, and most of the people use this technology to store and compute their data. The biggest issue is the security threats of cloud computing, and this research is focused on the security measures of those issues using advanced encryption algorithms. The research methodology focused on the studies of hashing and other cryptography encryptions and analyzed their implementation bu using different data sets. The results showed that Encryption algorithms symmetric, hybrid algorithms, hashing, and asymmetric algorithms are very useful to secure data of cloud from stealing.

# Methodology

## Research Design

Hashing is one of the complex topics in the field. The methodology which was used to create this paper was the qualitative methodology. Qualitative methodology is one of the most advance tool and technique which involves completing research. It is important to understand that there is a proper need fora brief analysis on which the content which has already been publishing was studied to understand the subject. There are four types of qualitative methodology which were used in the paper. It is important to understand that to complete the research, there is the need methodology design, which helps in identifying the problems regarding the technology(Schoonenboom, 2017).

One of the main reason to write this paper was to identify the issue which was involved in the problem. There are four types of techniques that have been used in qualitative technology. It is important to understand there all four types of tools helped to complete this research. The most common type of qualitative research is phenomenology. This type of research involves in development of the brief theory. Furthermore, it can be said the qualitative methodology is one of the helpful tools for the development of the research(Schoonenboom, 2017).

## Research Approach

The research which has been conducted is has been used as the approach of the subjective analysis. Remaining in the domain of the research question, this paper was complete. It is important to understand new and different techniques for the research have been utilized. Multiple research papers were analyzed to complete the research. The subjective methodology allows the user to understand the correct technique of developing subjective research. The subjective research approach helps the user to understand the proper functions of the paper, and it allow the user to evaluate the subject critically. This is one of the best tools for discovering the issue of the subject(Leavy, 2017).

A good strategy may develop leads to good results. Defining a procedure before starting the paper is the best policy. Before the research was started the paper review of the subject with the right references is necessary, so it is compulsory to gather all the relevant reference before your start to examine the subject. Reliable information has to be obtained from reliable sources. What decides them, that they are reliable is your methodology by investigating their researchers. A method is simply a research tool. Methodology justifies why a particular has chosen the specific method to obtain the right results(Leavy, 2017).

Remaining in the domain of the research question, it was discovered that hashing one of the complex issues. Anti-theft has become a cyber threat to the user. Encryption is the best techniques to make the password more secure for the user, but during the research was observed that hacker has been much strong to crack the passwords. It is important to understand that there are several tools and techniques to make the password more secure. Using the subjective methodology of multiple research papers and articles, it was observed that hashing is one of the best techniques to make the password more strong(Cao, 2020).

During the research, it was also observed that hashing is one of the best techniques of encrypting the password, and it has been observed that decryption of the password is not easy. The collection of the data was done through multiple sources that involved many different studies. It is important to understand that there is a brief need for the methodology to help and allows the user to understand the subject in such a manner that all the issues are discovered properly.

To complete the research, it was discovered the literature review was done on several topics. This is one of the subjective research approaches which helps to explain the paper more clearly. There are two types of methodology which are often use in the paper. The methodology and procedure of a research paper define the quality of the paper how accurate the information provided by individual supports the context with reliable sources. It can be said that both of these are techniques which have been explained are helpful for the individual to write research efficiently(Leavy, 2017).

# Result

The result can be defined as the finding of the research. The data which has been collected is based on the solution of the problem, and then it is converted into the information on. Results can be explained as the obtain solution to the problem. It has been observed that there is a need for a proper understanding of the problem which has been identified in the research. Several and multiple articles were studied to find a solution to the problem. During the research, it was observed that people were facing a lack of security, and their passwords were easily cracked. Hashing is the technique that is used to protect passwords, and it has been used widely.

# Discussion

The implication of usage of technological resources has extended the bases of the threat posed to the safety measures of the sensitive data (Álvarez, Andrade, & Zamora, 2018). These are the measures that are carried out in the course of analyzing the propensities which are to strengthen the security and maintain a stance of protocol and privacy for the users. The establishment of sensitive database protection needs to be established, and it is not possible without proper mechanisms of security.

**Outcomes**

The findings of the result showed that cryptographic algorithms provide data confidentiality, authentication, protection, integrity, and non-repudiation (HoudaFerradi, 2016). Hashing and asymmetric cryptography are the most effective techniques for data protection, and they make it difficult for intruders to enter into the data. The previous literature also indicated that these techniques surely reduce data theft inside the companies by encrypting data into different string locations. The subjective approach of our research provides a good description and implementation of Hashing and Asymmetric.

The outcomes of the research suggested that the relevant targets are mostly the internal enterprise and production networks from where the sensitive and secret data can be accessed. Our results showed that these new algorithms could make password theft impossible for hackers by extending the network protocols by approved and advanced security mechanisms. The protocols and algorithms cannot be reversed once integrated the mechanism into the enterprise and effective infrastructures. These techniques also address PKI and security measures to cloud technology, where users get a more secure data interface.

In this paper, we argue in favor of the implementation of hashing and asymmetric cryptography. People are demanding more effective security measures for Data Storage, Intellectual Property Rights Protection, Regulatory Compliance, Infrastructure Downtime, Data Backup, Reliability, and Redundancy, which can be possibly protected by the Advanced Encryption Standard used in asymmetric encryption. Most of the previous research had a big scope in the field of IT and was approved by the experts. Their techniques and results are still in use of federal agencies and national customer services. Our research has analyzed the work of previous researchers and presented the outcomes with more efficiency and reliability.

**Advantages**

We have found that hashing provides great protection for confidential data because it is impossible to figure the input from a specific output in data. It provides authentication by providing message integrity checks and checksum. Hashing generates the pseudorandom numbers and digital signatures and verifies them for data confidentiality. Hashing provides more data integrity, but Asymmetric also uses wise data scrambling, which increases the safety of passwords and information. The method uses different keys for encryption and decryption, which makes it difficult to decrypt the data. The private key is handed over to the main person or owner, which should not be accessed by other people, and public keys are handed over to trustees (Sardar, 2020). The creation of digital signatures and numbers helps the company to protect the data flow like in TLS protocol. The findings of the research showed great results in the cryptography algorithms.

**Limitations**

These algorithms are of great significance, but results also showed some limitations of these methods. Adoption of the indigenous and poor algorithms can become the reason for data breach and data theft. In asymmetric, the biggest threat comes from the distribution of keys. Although the private and public keys have different functions to protect the confidential data giving the public key to a non-trusted worker or another person can cause data breaching (SSD, 2018). All the information on data encryption can be accessed from public keys, and it will make it easy for the hacker to enter into the company’s server. In the case of hashing, it is impossible to reverse the hashed data as long as the algorithm and function used in hashing are strong (Defuse Securit, 2019). The hashing data can be accessed and broken by using the same hashing collision. If the password or algorithm is weak in the implementation of hashing, the intruder will access the hash data and crack the code for personal use.

**Scope**

Hashing and Asymmetric cryptography are surely the best means to stop data theft. Although they have their limitations, if they are implemented in the right way by using the right set of algorithms and data signatures, they can stop major data breaching. The findings of the research show the positive effect of cryptographic algorithms and recommended that these techniques should be used to protect confidential data. These methods are more reliable and integrated and, again, can benefit a lot if implemented by the right set of rules. The scope of the study is good, as the previous literature was professionally reviewed. The findings of the researchers are molded and enhanced in this research with an effective framework and qualitative approach. This data set and results can be used to help the community to overcome the security threats and can also be used in several state and federal agencies for security measures because most of our literature review was approved and appreciated by higher authorities and experts.

**Conclusion**

Cybersecurity is an emerging issue in this advanced and modern world, and people demand security measures to protect their data from stealing. Many federal and government departments face real cyber threats through which their confidential and secret information can be jeopardized. Hashing and asymmetric are the best cryptocurrency algorithms that can be used for the protection of passwords and user data of the users. This research covered the importance and implementation of these two algorithms and recommended its use for security measures against data theft.

# References

Álvarez, R., Andrade, A., & Zamora, A. (2018). Optimizing a password hashing function with hardware-accelerated symmetric encryption. *Symmetry*. 705.

Álvarez, R., Andrade, A., & Zamora, A. (2018). Optimizing a Password Hashing Function with Hardware-Accelerated Symmetric Encryption.

Cao, W. F. (2020). A review of hashing methods for multimodal retrieval. *IEEE Access* *, 8*, 15377-15391.

Defuse Securit. (2019, June 5). *Salted Password Hashing - Doing it Right.* Retrieved July 26, 2020, from Crack Station: https://crackstation.net

HoudaFerradi. (2016). Integrity, authentication and confidentiality in public-key cryptography. *Cryptography and Security PSL Research University* .

Leavy, P. (2017). *Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches.* New York, New York: Guilford Publications.

Leavy, P. (2017). *Research design.*

Omara, F. A., & AbdElnapi, N. M. (2016). A hybrid hashing security algorithm for data storage on cloud computing. *International Journal of Computer Science and Information Security* .

Raymond, V. J. (2017). Google drive based secured antitheft android application. . *In 2017 International Conference on IoT and Application* , 1-8.

Sapkota, A. (2015). *Pratical data security testing on virtual learning environment.*

Sardar, Z. (2020, April 30). *Cryptographic Algorithms.* Retrieved July 26, 2020, from Electronic Design: https://www.electronicdesign.com

Schoonenboom, J. &. (2017). How to construct a mixed methods research design. *KZfSS Kölner Zeitschrift für Soziologie und Sozialpsychologie, , 2* (69), 107-131.

SSD. (2018, November 11). *A Deep Dive on End-to-End Encryption: How Do Public Key Encryption Systems Work?* Retrieved July 26, 2020, from Survilliance Self-Defense: https://ssd.eff.org

Toapanta, S., Astudillo, K., & Gallegos, L. (2020). Appropriate Security Algorithms to Mitigate the Risks in a Database of the National Customs Service of Ecuador. *Proceedings of the 2020 the 4th International Conference on Information System and Data Mining* , 89-95.