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

**Research Methods**

Student Name : Sagarika Nagaraj

Student ID : 17061633

Table of Contents

[Abstract 1](#_Toc46767486)

[Introduction 1](#_Toc46767487)

[Research Question 2](#_Toc46767488)

[Aims and Objectives 2](#_Toc46767489)

[Background 2](#_Toc46767490)

[Methodology 4](#_Toc46767491)

[Research Design 4](#_Toc46767492)

[Research Approach 5](#_Toc46767493)

[Result 6](#_Toc46767494)

[Discussion 6](#_Toc46767495)

[References 10](#_Toc46767496)

**ABSTRACT**

Data theft is basically an act of stealing data that is stored on computers or other devices from an unknowing victim with the aim to hack personal or confidential information. The impact of data theft is that when a hacking attempt is made, a business would be unable to use their software or devices. The prime focus of the research is to highlight the domains of maintaining different methodologies that are established in order to provide considerations in case of data protection. This measure of protection is the consideration that is developed on the bases of aligned infrastructure and the mechanisms of hashing and asymmetric course of interactions are to be weighed. Aligned infrastructure basically consists of the details of architecture, reliability, and security. The alignment requires skills in delivery and support areas as well as in the areas of flexibility and agility. In this paper, we will look at different methodologies for the protection of data. The Password-Based Key Derivation Functions (PBKDF) is carried out in this study of the functions through which the passwords are transmitted into secret keys. This process tends to maintain the fixed size cipher function of the operation. The PBKDF is also called Hashing. The measure of Asymmetrical cryptography also provides the bases of antitheft measures.

# INTRODUCTION

Digital security could be working out of ensuring PCs, workers, cell gadgets, electronic frameworks, sites, and information from noxious attacks. It is likewise called security or data assurance that is electronic.(Kaspersky, 2020) Encryption might be the manner by which data is changed into a key code that conceals the subtleties' genuine importance. The innovation of encoding and data that is decoding called cryptography. In processing, decoded data can be called plaintext, and scrambled data is named cipher text. (Margeret, 2020)

Hashing is the change of a progression of numbers into a regularly shorter fixed-length worth or key that speaks to the grouping that is beginning. Hashing is utilized to record and recover things in an information base it using the worth that is starting it is quicker to discover the item using the diminished hashed key than to discover. (Margaret, 2020). Encryption is a capacity that is two-way what's scrambled are decoded alongside the key that is fitting. Hashing, in any case, is only a capacity that is single direction scrambles text that is plain produce a unique message digest. Having a satisfactorily planned calculation, it is extremely unlikely to switch the hashing system to uncover the secret phrase that is unique. (GCN, 2020)

Hashing is certainly a calculation done on information like a message or record to deliver a volume called a hash (alluded to as a checksum). The hash is utilized to check that information isn't adjusted, messed with, or ruined. Spot another genuine way, you will approve the information has looked after uprightness. (Glossary, 2020)

**RESEARCH QUESTION**

Can the data be protected by implementing the applications of hashing and asymmetric encryption?

**AIMS AND OBJECTIVES**

There are a number of practices by using which we can protect our data from stealing. In this paper, we are focusing on the applications of hashing and asymmetric encryption. This research will highlight the following aims and objectives:

• The evaluation of different securing measures for data from theft.

• Analysing the security of data through hashing.

• Assessment of security of data through asymmetrical encryption.

**BACKGROUND**

The foundation of this paper is created in such a measure that the appraisal of the various executions of insurance is evaluated from the preference of looking after antitheft. The foundation of security did the course of adjusted methods that is important for the insurance grounds (Toapanta, Astudillo, and Gallegos, 2020). The picked strategy isn't just zeroing in on the outline that is assessed throughout surveying yet additionally breaking down the premise which is continued according to the formative examination and the qualifications of the conduct of the control. These are the position of the methodological bases, which will give the portrayal of examination through the upkeep of systems that are important to continue the course of information base security and assurance.

As the innovations are introduced for better use and protection of data, new risks and threats are also coming into the market with the advancement. 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 lots of people lost their money which is deposited in the banks. According to reports, approximately 100,000 Australians personal information has been exposed in a hack affecting Westpac bank. Hacking of ATM’s passwords has become common nowadays, and people are losing their money and assets. New cyber security 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 with the help of encrypting and decrypting the data techniques. 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 provides data authentication and integrity. Hashing makes the different string indexes for each data values, and that data cannot be reversed back to its original value.

Hashing and Asymmetric techniques are now commonly used because of its reliable cryptography techniques. 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 these kinds of crimes. The government is paying more to the tech companies to upgrade these techniques for better control of data protection and circulation.

Hashing is the building block of advanced cryptography. A hash function is basically a cryptographic algorithm and it is used to transform large size data into small fixed-size data. The output data of the hash algorithm is known as a digest or hash value. The general operation of the hash function does not need a key and operates in a single-way manner. Asymmetric algorithms are generally known as “PUBLIC KEY” algorithms. This algorithm basically uses two mathematically associated keys which are known as public and private keys. One of them is used for encryption of data while the other is used for decryption of data.

# Rafael Alvarez 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 cyber security 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 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 threat on cloud computing, and this research is focused on the security measures of those issues using advanced encryption algorithms. The research methodology focuses on the studies of hashing and other cryptography encryptions and analyse their implementation by using different data sets. The results demonstrate 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 is used to create this paper was the qualitative methodology. Qualitative methodology is one of the most advanced tools and techniques that help incomplete research. It is important to understand that there is a proper need for a brief analysis of which the content has been already published and these studies are analysed to prepare this study. There are four types of qualitative methodology which uses in the paper. The methodology is a necessary part that helps in identifying the problems regarding technology (Schoonenboom, 2017).

One of the main reasons to write this paper is to identify the issue which is involved in the problem. There are four types of techniques that have been used in qualitative technology. It is important to understand these 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**

It is important to understand new and different techniques that have been utilized in the research. Multiple research papers were analysed to complete this research. The methodology allows the user to understand the correct technique of developing research. The research approach helps the user to understand the proper functions of the paper, and it allows the user to evaluate the subject critically. This is one of the best tools for discovering the issue of the subject (Leavy, Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches., 2017).

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 method is chosen to analyses this point of view and why this method us correct to obtain the right results (Leavy, Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches., 2017).

Remaining in the domain of the research question, it was discovered that hashing is 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, it was observed that hacker has been much strong to crack the passwords. 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 and safe (Cao, 2020).

During the research, it was also observed that hashing is one of the best techniques for encrypting the password, and it has been observed that decryption of the password is also 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 help to explain the paper more clearly. There are two types of methodology which are often used 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 proved to be helpful for the individuals to write research efficiently (Leavy, Research design., 2017).

**RESULT**

The result of the research can be obtained with the help of the findings of the research. The data which is collected and used in the research is based on the problem’s part and then the data is converted into information. Results are the obtained solutions to various problems that discussed in the paper. Various and many articles were studied just to get the solution to the problem. It was observed that people are facing a lot of issues and security and their passwords are easily hacked. Hashing is one of the most important techniques to protect passwords and this technique is used widely.

**DISCUSSION**

A proper mechanism is a need for securing the passwords and for securing sensitive data from threats (Álvarez, Andrade, & Zamora, 2018).

**OUTCOMES OF HASHING AND ASYMMETRIC CRYPTOGRAPHY**

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 area and steal data. The previous literature also indicated that these techniques surely reduce data theft within the premises of 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 SSD, 2018).

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 (Houda Ferradi, 2016).

In this paper, we argue in favour 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. This research has analysed the work of previous researchers and presented the outcomes with more efficiency and reliability (Leavy,2017).

**ADVANTAGES OF HASHING AND ASYMMETRIC CRYPTOGRAPHY**

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 to the main person or owner, and this 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 OF HASHINGS**

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 hackers to enter 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 OF HASHING AND ASYMMETRIC CRYPTOGRAPHY**

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 modeled 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 reviews were approved and appreciated by higher authorities and experts (Cao, 2020).

**CONCLUSION**

Cyber Security 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 crypto currency 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. and Zamora, A., 2018. Optimizing a password hashing function with hardware-accelerated symmetric encryption. *Symmetry*, *10*(12), p.705.

Cao, W., Feng, W., Lin, Q., Cao, G. and He, Z., 2020. A review of hashing methods for multimodal retrieval. *IEEE Access*, *8*, pp.15377-15391.

Abdullah, M., 2016. SPM System Cybersecurity-Defuse Security. Salted Password  
Hashing - Doing it Right. <https://crackstation.net/hashing-security>.

Ferradi, H., 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*. Guilford Publications.

AbdElnapi, N.M., Omara, F.A. and Omran, N.F., 2016. A hybrid hashing security algorithm for data storage on cloud computing. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(4).

Raymond, V.J. and Sushmitha, E., 2017, May. Google drive based secured anti-theft android application. In *2017 International Conference on IoT and Application (ICIOT)* (pp. 1-8). IEEE.

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. and Johnson, R.B., 2017. How to construct a mixed methods research design. *KZfSS Kölner Zeitschrift für Soziologie und Sozialpsychologie*, *69*(2), pp.107-131.

Shah, M., Aditya, A., Bindra, D., Omkar, V.S. and Seervi, A., Providing a Secure, Reliable and Decentralized Document Management Solution Using Blockchain by a Virtual Identity Card. *International Journal of Computer and Information Engineering*, *14*(1), pp.24-28.

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