Project Proposal

Paper Title:

Database security with encryption

(Number plate recognization with encrypted data)

Group Members:

Group – 13

Chaitanya Chowdary Paladugu – ria23

Sriram Putta – dse33

Ganesh Tummala – eek26

Nithish Patibandla – hgb42

**Task 1** (10 points) Give a high-level overview (like a summary) of the key contributions of the paper that your team has picked?

Overview:

< Summarized description of the paper>

Nowadays, security plays a significant role in all aspects of the world. Here there are two major parts one is authorization, and the other is authentication. Authorization means whether the person has the right to access the data or not, whereas authentication means username/password. The encryption and decryption of plain text were necessary. Before sending the data into the database, we encrypt it and then save it in the database. Whenever we want to retrieve it, we decrypt the encrypted data using keys.

By using encryption, the intruder cannot access the raw data. Usually, database encryption can be done in two different ways, One is encryption, and another is hashing. In encryption we use DES, RC2, AES\_128, AES\_256, RSA encryption approaches. About the hashing, once data is hashed, We will not be able to change the hashed data back to plain text. In hashing, there are different types of hash functions we have seen in this paper, for example, MD4, MD5, SHA, and SHA-1.

From this paper, we have also seen there are three primary types of categories; The first one is standalone encryption approaches, and the second is hybrid, for example, RSA and IDEA approach. This hybrid approach enhances the security; the intruder cannot access the raw data, and third is hashing; in this, we use the MD5 hashing function, mostly used for password encryption, and can modify the information for future enhancement.

Intellectual Merit:

< Key Takeaways from the paper>

Understanding the importance of the research in today's world, everything we use, like emails, and social networking app data, is stored in a database, how an intruder can easily access the data from the database. We will understand how authentication and authorization are two significant parts of data safety and how they fall short. From this paper, we can understand various encryption schemes and limitations. We understand the encryption process and the decryption process that happens in the database. We understand how the differences in the workflow of encryption and hashing. We understand the differences and limitations of Standard encryption approaches, Hybrid approaches, and Hashing. This paper will be able to compare and see the results of different approaches that we use on the data and their merits and demerits. After going through the paper, we have decided to implement one of the encryption approaches in an application.

Task 2 & 3

Proposed Work and Methodology

**Task 2:** (5 pts) Describe which specific topic from the paper you are investigating in further detail over the next two months and why you picked that topic? Describe how it ties to the topics that we have covered in the class? Which application areas can the idea that you have chosen to be applied to?

Most modern companies face many data breaches, so if a data breach has occurred, all our data will be in the wrong hands. To avoid such cases, we are using this project as an example to present an approach that will be helpful in the outside world. From the paper, we have decided to use the RSA encryption approach after studying and understanding different encryption approaches. RSA encryption is one of the critical encryption approaches in the encryption approaches, and RSA has two different types. RSA and RSA with asymmetric. We will implement an application that can use a machine learning algorithm to get data, and once we get the data from it, we will use encryption on the data, which encrypted data will store in the database.

In class, we have heard different approaches to encryption. Therefore, we as a team want to implement one of the encryption approaches (RSA) in real-world applications, which helps to understand how companies use this. Furthermore, implementing an application allows us to overcome different problems and understand our approach more.

For example, if an intruder acts the company database to access the main gate vehicle data entry. In today's world, all the data is computerized, and information is stored in a database. If an intruder acts on the database to access such data, our application will help in such cases. Our application will not store any plain text directly in the database. Instead, our application will help keep the encrypted data in the database. So even if an intruder acts the database, the intruder will not be able to use that data any further.

**Task 3:** (5 pts) As part of the final presentation, you will be required to demonstrate software for one idea presented in the paper or a new idea that you may have based on what you learned from the paper? For the project proposal phase, describe which idea you will be picking and how you plan on approaching this task?

After we had read the paper, we decided to implement an application about how to do encryption on the data. We have decided to use machine learning and encryption to add up the complexity after much surfing and reading about the implementations of encryption databases. In addition, we have researched how companies avoid data breaches, from which we thought of implementing an application. Finally, take a real-world example of implementing a machine learning project with encryption data. It helps us gain more knowledge about the approach we are proceeding with. For the next two months, we plan on implementing a machine-learning project, but for the data's security, we are encrypting the database. We have studied different encryption approaches from which we have decided to use RSA.

We have decided first to build a basic encryption model for the data, and we will also use decryption to check whether the output we have is correct or not. Once we have the basic encryption model ready, we will move on to the project's next phase, building a machine learning model that is number plate recognization. Once we get the data from the recognization model, we usually send them directly to the database (CSV file) for storage. Still, we will add encryption before sending the data to the database (CSV). This helps us to have only encryption data in the database.

The main challenge we will be facing is implementing an encryption approach. Adding an encryption approach to desired output from the machine learning model and sending the encryption data to the database (CSV).

Website URL:

<https://www.researchgate.net/publication/282925678_Database_security_using_encryption>