IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DEVELOPMENT OF CAR LOAN WEB APPLICATION USING CRYPTOGRAPHY

[1]Prof. A. P. Kadam , [2]Divya Gaikwad , [3]Sejal Gholap, [4]Amruta Hedgire, [5]Sakshi Jagtap
[1]Professor, [2]Student , [3]Student , [4]Student , [5]Student
1Computer Department , 1BVCOEW, Pune , India

***Abstract*: -** In the digital age, web applications that facilitate vehicle loans must prioritize the security of sensitive financial data. This abstract discusses how cryptography is used to strengthen the security of an auto loan web service, specifically the implementation of AES (Advanced Encryption Standard) for data encryption and Bcrypt for password protection. AES protects private information by encrypting it using a secret key and protecting it from prying eyes. Bcrypt, on the other hand, secure hashes and stores user passwords in a one-way format to protect them. This strategy strengthens the application against data breaches, guarantees the privacy and security of user information, and builds credibility and confidence in the online world.

Keywords: Cryptography , AES (Advanced Encryption Standard) ,Bcrypt ,Data Encryption , Password protection , Sensitive information.

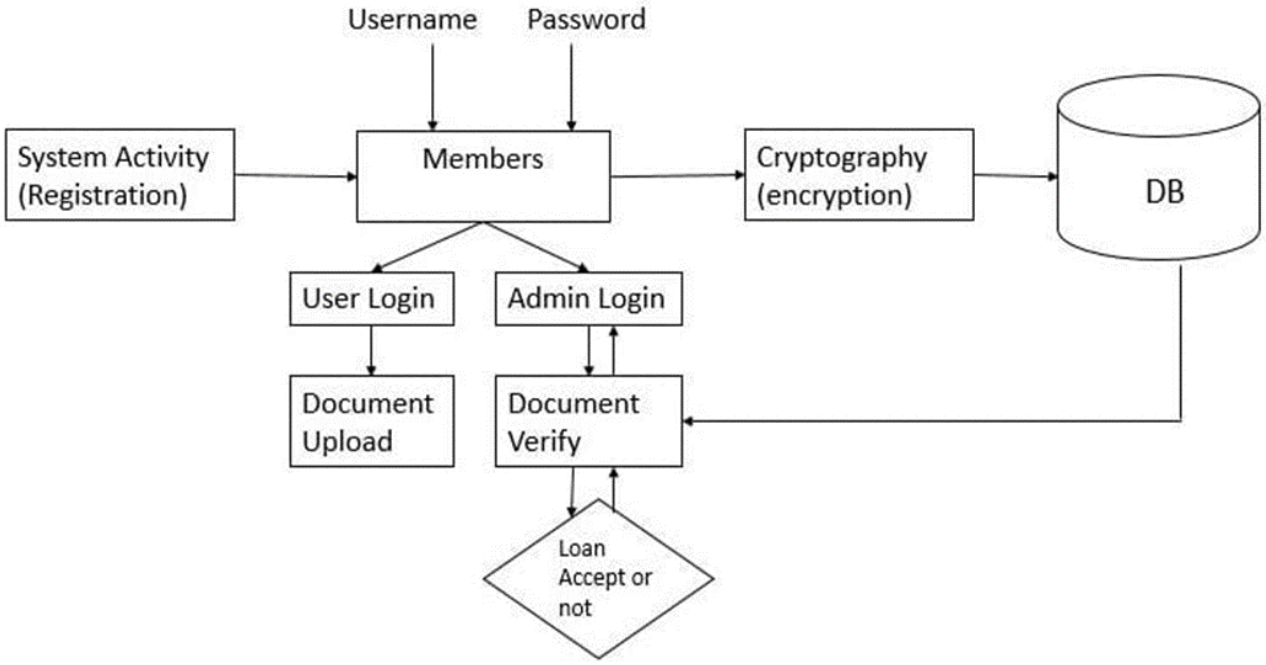
1.INTRODUCTION

The security and privacy of sensitive financial data must be guaranteed in the current digital era. Securing this information is essential when it comes to a web application for vehicle loans where customers disclose personal and financial data. AES (Advanced Encryption Standard) and B crypt are two crucial cryptographic tools for improving the security of such applications. Because of its strong security properties, AES is a symmetric-key encryption technique that is frequently used. Data is encrypted and decrypted using a secret key, guaranteeing confidentiality. Sensitive data, including social security numbers, information about one's income, and contact details, can be encrypted using AES before being saved in a database when used in the context of a web application for a car loan. Through encryption, the risk of unauthorized access is greatly reduced since even if the database is compromised, the attacker would need the secret key to access the data. On the other side, B crypt plays a crucial role in safeguarding user passwords. Passwords are safely stored in hashed format using a one-way cryptographic hash function. In the car loan online application, when a user opens an account or modifies their password, B crypt takes that user's password, hashes it, and then stores the hash in the database. As a result, the original passwords are never kept on file, and even if the database is compromised, attackers will find it difficult to decode the hashed passwords.

2. LITERATURE REVIEW

1. Mohammed M. Alani, Applications of Machine Learning in Cryptography: Machine learning is used in the domains of cryptography and cryptanalysis. a wide range of issues and advancements, including cryptographic applications such as machine learning-based cryptosystems, encrypted traffic classification, and cryptanalysis of encryption methods. The routes this area will go in the future are discussed, including the application of machine learning to create new cryptosystems, privacy-preserving training, cryptanalysis methods, and machine learning-enhanced existing techniques. Overall, the study emphasizes the growing importance of machine learning in improving information and network security, as well as the possibility for additional research and development in this field. It is a useful tool for comprehending how machine learning and cryptography interact.
2. Abdalbasit Mohammed, A Review Paper on Cryptography: It describes how cryptography came to be and how it became a crucial component of contemporary information security. The study emphasizes the value of cryptography for network and computer security as well as its adaptability to deal with new threats. The study discusses numerous cryptography methods, both symmetric and asymmetric, and emphasizes their significance in protecting data during various communication processes. It recognizes that social networks and e-commerce have a significant impact on data generation and that secure data transport requires sophisticated encryption algorithms. The authors address both traditional techniques such as the Caesar Cipher and contemporary ones like as stream ciphers, block ciphers, hash functions, and public key systems, emphasizing the need for cryptographic algorithms to be robust and easily available to the general public. The research also examines the validity of message authentication through digital signatures.
3. Jollanda Shara, Some Applications of Machine Learning in Cryptography: The research emphasizes that machine learning and cryptography have a lot in common, especially when it comes to processing massive volumes of data and navigating large search areas. It emphasizes how machine learning, with its variety of methodologies, has a lot of potential for use in cryptanalysis and cryptography. The use of machine learning to improve the effectiveness and efficiency of cryptographic systems is the main idea. It describes the use of machine learning to problems including classification, regression, learning associations, unsupervised learning, and reinforcement learning while highlighting the relevance of these techniques to cryptographic settings. In particular, it covers the application of machine learning methods to perform cryptanalysis and even generate private cryptographic keys via open channels.
4. Anggit Permana, Siswanto, and Rizka Tri Alinse, A Decision Support System for Giving Used Car Loans Using the AHP Method at PT. Batavia Prosperindo Finance Tbk: The Analytical Hierarchy Process (AHP) is the researchers' preferred method for addressing the problem. AHP is a multi-criteria decision-making technique that aids in ranking distinct alternatives according to multiple criteria. In this instance, it assists in determining a person's eligibility for used car loans. The value of technology in expediting and enhancing the decision-making process is highlighted. It reveals that PT. BPF Bengkulu had previously employed a manual method, which might have resulted in mistakes in computations and data reading. The AHP approach is well explained by the authors, who also discuss how it might be utilized to address the problem of used automobile loan approvals. The findings of their study demonstrate that using predetermined criteria and sub-criteria, they were able to assess loan eligibility using a final score.
5. Jeannie Marie Paterson and Nicola Howell, Everyday Consumer Credit: An Overview of the Australian Law Regulating Consumer Home Loans, Credit Cards, and Car Loans: This paper provides a thorough overview of consumer credit protection law and regulation in Australia, focusing on specific credit products like home loans, credit cards, and car loans. It also analyzes the interaction between various legal regimes governing consumer credit, including the National Consumer Credit Protection Act 2009 (NCCP Act) and the National Credit Code (NCC). The study emphasizes the critical significance of outlawing activity that misleads or deceives consumers, damaging their autonomy and freedom of decision-making. Additionally, it emphasizes the need of giving customers correct information because informed customers are better able to defend their rights. The authors talk about the difficulties that required disclosure has in influencing customer choices, especially in complicated financial transactions. They make reference to the constraints of disclosure and the role of behavioral economics in enhancing customer outcomes.

3. SYSTEM ARCHITECTURE



In the development of a web-based car loan application, cryptography plays a pivotal role in safeguarding the confidentiality and security of sensitive user data. The system comprises two distinct login portals: one for users and the other for administrators.

1.User Registration and Profile Management: The initial step involves user registration, where individuals can create their profiles by providing personal information and uploading the necessary documents. To ensure data security, all the information and documents submitted by users are immediately encrypted using cryptographic techniques before being stored in the database. This encryption process converts the data into an unreadable format, rendering it highly secure.
2.Administrator's Role: The encrypted user data is exclusively accessible to the administrator. The administrator logs into their own secure portal, where they can view and manage the incoming user data.
3.Document Verification and Loan Approval: At this point, the administrator's role comes into focus. They have the capability to decrypt the encrypted user data, thereby gaining access to the original information and uploaded documents. The administrator can then conduct a thorough verification process, examining the provided documents and assessing the user's information. This verification process is a critical step in determining whether to approve or deny the loan application.
4.Data Security and Confidentiality: The use of cryptography in this process ensures that even if unauthorized access were to occur, the stored user data would remain unintelligible. The encryption and decryption keys are securely managed, preventing data breaches and unauthorized access.

4. CONCLUSION

As a result, we will use cryptography to create a web-based vehicle loan application. We'll use encryption techniques like 1.AES (Advanced Encryption Standard). 2.Bcrypt 3. A encrypted database. As a result, a secure data encryption web application for a vehicle lending system can be implemented. In conclusion, the development of a car loan web application incorporating Advanced Encryption Standard (AES) cryptography represents a significant stride towards enhancing the security and privacy aspects of online financial transactions. By implementing AES, a robust and widely recognized encryption algorithm, the application ensures the confidentiality and integrity of sensitive user information, such as personal and financial data. This not only instills trust among users but also aligns with contemporary cybersecurity standards. The utilization of cryptography in the form of AES in the web application adds an additional layer of protection, mitigating the risk of unauthorized access and potential data breaches. As technology continues to advance, prioritizing security measures, such as AES encryption, becomes imperative in safeguarding the confidentiality and integrity of user data in financial transactions, reinforcing the viability and reliability of the car loan web application in today's dynamic digital landscape.

5. FUTURE SCOPE

1. **Continuous Security Improvements:** Ongoing advancements in AES and related cryptographic algorithms will provide opportunities to enhance the security features of the application. Regular updates and improvements can be implemented to stay ahead of emerging threats.

2. **Quantum Computing Resistance:** As quantum computing technologies advance, the potential for breaking traditional cryptographic algorithms increases. Exploring and integrating post-quantum cryptographic techniques will be crucial to ensuring the long-term security of the car loan web application.

3. **Multi-Factor Authentication Integration:** Future developments could involve the integration of multi-factor authentication methods, such as biometrics or hardware tokens, to augment the security provided by AES encryption. This extra layer of authentication would further fortify access controls.

4. **Enhanced User Privacy Measure**s: Research into privacy-preserving cryptographic techniques can lead to the development of methods that allow the application to collect and utilize necessary information for loan processing without compromising the user's sensitive data, thus improving overall privacy measures.

5. **Interoperability and Standardization:** Future work can focus on developing standards for cryptographic implementations in financial applications, promoting interoperability and ensuring that the car loan web application can seamlessly integrate with evolving technologies and security protocols.

6. **Machine Learning for Threat Detection:** Integrating machine learning algorithms can enhance the application's ability to detect and respond to emerging cybersecurity threats. This proactive approach can help in identifying anomalies and potential security breaches before they escalate.

7. **Global Regulatory Compliance:** Given the dynamic nature of regulatory frameworks, the future scope involves continuous adaptation to comply with evolving data protection and financial regulations globally. Staying abreast of regulatory changes will be crucial for the application's long-term success.

6. REFERENCES

[1] Mohammed M. Alani. 2019. Applications of Machine Learning in Cryptography: A Survey. 1, 1 (February 2019), 8 pages. https://doi.org/10.1145/3309074.3309092

[2] Mohammed, Abdalbasit & Varol, Nurhayat. (2019). A Review Paper on Cryptography. 1-6. 10.1109/ISDFS.2019.8757514.

[3] Shara, Jollanda. (2020). Some Applications of Machine Learning in Cryptography

[4] Permana, A., Siswanto, S. Alinse, R.T.. (2021). A Decision Support System for Giving Used Car Loans Using the AHP Method at PT.Batavia Prosperindo Finance Tbk Jurnal Komputer, Informasi dan Teknologi, 2 (2). DOI: https://doi.org/10.53697/jkomitek.v2i2

[5] Paterson, Jeannie & Howell, Nicola (2018) Everyday Consumer Credit Overview of Australian Law Regulating Consumer Home Loans, Credit Cards and Car Loans: Background Paper 4. The Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, Australia.

[6] S. Shuai, D. Guowei, G. Tao, Y. Tianchang and S. Chenjie, "Modelling Analysis and Auto-detection of Cryptographic Misuse in Android Applications," 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing, Dalian, China, 2014, pp. 75-80, doi: 10.1109/DASC.2014.22.