CLIENT RESPONSE PLATFORM

[1] Mrs. T.Sai Santhoshi,[2] G.Varsha,[3] G.Karuna,[4] G.Lourdu Praveen Kumar,[5] G.Tharun
[1] Assistant Professor,[2345] B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

ABSTRACT

Developing effective mechanisms for feedback collection in learning environments is particularly important at the frontiers of new knowledge .Valuing and asking for feedback has recognised benefits for both staff and students. For Staff to provide information for course design to further develop teaching skills as well as to provide better service to the students. For Students to feel valued and 'listened' to have ownership in their own learning to develop reflective thinking to be better informed inselecting a course/module . The online feedback collection systems, described in this project are two such applications for collecting feedback through a web interface. Intended to support feedback collection in educational environments

.ITC – feedback system collects feedback from users about the services offered by for Information Technology and Communication wing (ITC) of NITC. Faculty- feedback system is intended to collect feedback about faculty, from students.

I. INTRODUCTION

Getting the right feedback at right time is of at most importance, for any organization or faculties of an institution. Getting the feedback from the users will help an organization or faculty to provide better services to the users or students. Ongoing interaction with users can help improve the efficiency of an organization, and enable them to provide better service to the users. Collecting feedback from the users is very important thing for any organization.

Until now, feedback collection process is conducted manually, using printed forms. All that has changed with the computer network as well as World Wide Web, making communication far easy. It is very easy to collect feedback about an organization, or about the staff of an institution through a web-based system. Valuing and asking for feedback has recognized benefits for both staff and students in an institution. For Staff to provide information for course design to further develop teaching skills to match learning to learners needs to support bids for funding teaching projects For Students to feel valued and 'listened' to have ownership in their own learning to develop reflective thinking to be better informed in selecting a course/module For All to enhance relationships and define roles to provide a 'positive' teacher/student partnership, which in turn has more chance of ensuring high quality teaching, thereby meeting learners' needs to establish learning objectives, and measure the extent to which they are met to inform executive action, policy developments and resource allocation as part of quality assurance procedure Feedback should be encouraged to be positive as well as giving suggestions concerning areas that could be enhanced. This project aims to develop two online feedback collection systems, one system is intended to collect the feedback from users of Information Technology and Communication (ITC) wing of National Institute of Technology, Calicut. Second part of the project is to develop an online feedback collection system for collecting feedback about the faculty, from the students.

II. LITERATURE SURVEY

1. TITLE: Use of Digital Signature with DiffieHellman Key Exchange and AES Encryption Algorithm toEnhance Data Security in Cloud Computing

AUTHOR: PrashantRewagad, YogitaPawar.

ABSTRACT: Cloud computing is the apt technology for the decade. It allows user to store large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, and authentication is encountered. In order to get rid of the same, a variety of encryption algorithms and mechanisms are used. Many researchers choose the best they found and use it in different combination to provide security to the data in cloud. On the similar terms, we have chosen tomake use of a combinationof authentication technique and key exchange algorithm blended with an encryption algorithm. This combination is referred to as “Three way mechanism” because it ensures all

the three protection schemeof authentication, data security and verification, at the same time. In this paper, we have proposed to make use of digital signature and Diffie Hellman key exchange blended with (AES) AdvancedEncryption Standard encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user's private key, which is confined only to the legitimate user. This proposed architecture of three way mechanism makes it tough for hackers to crack the security system, thereby protecting data stored in cloud. Cloud computing is the apt technology for the decade. It allows user to store large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, and authentication is encountered. In order to rid of the same, a variety of encryption algorithms and mechanisms are used. Many researchers choose the best they found and use it in different combination to provide security to the data in cloud. On the similar terms, we have chosen to make use of a combination of authentication technique and key exchange algorithm blended with an encryption algorithm.

TITLE: Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing.
AUTHOR: Uma Somani, Kanika Lakhani, ManishaMundra
ABSTARCTS
The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. Today, we have the ability to utilize scalable, distributed computing environments within the confines of the Internet, a practice known as cloud computing. Cloud computing is the Concept Implemented to decipher the Daily Computing Problems, likes of Hardware Software and Resource Availability unhurried by Computer users. The cloud Computing provides an undemanding and Non ineffectual Solution for Daily Computing. The prevalent Problem Associated with Cloud Computing is the Cloud security and the appropriate Implementation of Cloud over the Network. In this Research Paper, we have tried to assess CloudStorage Methodology and Data Security in cloud by the Implementation of digital signature with RSA algorithm.
TITLE: - Student Feedback System
AUTHORS: - G. Bhanukiran, K. N. V. Sree Vathsa, K. Venkat Ravi.
ABSTRACTS: - Student Feedback system is used to get the feedback from the students. It generates the reports for the faculty on the basis of given feedback by the students. The staff will be provided with separate usernames and password in order to check the results. The total report is visible to the people like chairman and principal. It contains the modules like student, faculty and admin. Admin is the responsible for creating a class and assigning the corresponding faculty to the class. Within short time we can get the performance of the faculty from the student point of view. There are 15 questions to evaluate the status of faculty and each question contains 5 options like Excellent, very good, good, Average and Poor.

TITLE: - Automated style feedback
AUTHORS: - Hannah Blau, Samantha Kolovson, W. Richards Adrion, Robert Moll
ABSTRACTS: - Student Feedback system is used to get the feedback from the students. It generates the reports for the faculty on the basis of given feedback by the students. The staff will be provided with separate usernames and password in order to check the results. The total report is visible to the people like chairman and principal. It contains the modules like student, faculty and admin. Admin is the responsible for creating a class and assigning the corresponding faculty to the class. Within short time we can get the performance of the faculty from the student point of view. There are 15 questions to evaluate the status of faculty and each question

contains 5 options like Excellent, very good, good, Average and Poor.

III. SYSTEM ANALYSIS & DESIGN

EXISTING SYSTEM

The existing method for collecting feedback about the faculty from the students makes use of printed forms on paper. Students write their feedback and submit it to the faculty. This is very time consuming and costly procedure. Preparing the printed form and collecting the forms back from the students is a time consuming procedure. Collecting the feedback from the students about the service offered by ITC is also such a time consuming and difficult procedure.

DISADVANTAGES

• Collecting the feedback from the students about the service offered by ITC is also such a timeconsuming and difficult procedure

• Preparing the printed form and collecting the forms back from the students is a time- consuming procedure.

PROPOSED SYSTEM

The Proposed system is a web based system. The user can login to the system with a valid ID and password, fill in an online feedback form and submit the feedback to the system. The administrator canlater analyze the feedback.

. The online feedback collection systems, described in this project are two such applications for collecting feedback through a web interface. Intended to support feedback collection in educationalenvironments . Feedback system collects feedback from users about the services offered by for Information Technology and Communication wing . Faculty-feedback system is intended to collectfeedback about faculty, from students.

ADVANTAGES

- The proposed online feedback collection system is a web based system. So valid users can access itfrom anywhere.
- This is a platform-independent system. So there is no need for installing any additional software on theclient systems.
- The new system issues the users , and asset of questionnaires. The user answers the question andsubmits this feedback.
- This is very effective, fast and cost-effective method for collecting feedback.
- The users, who give the feedback, are authenticated with a Login ID and password.

SYSTEM ARCHITECTURE

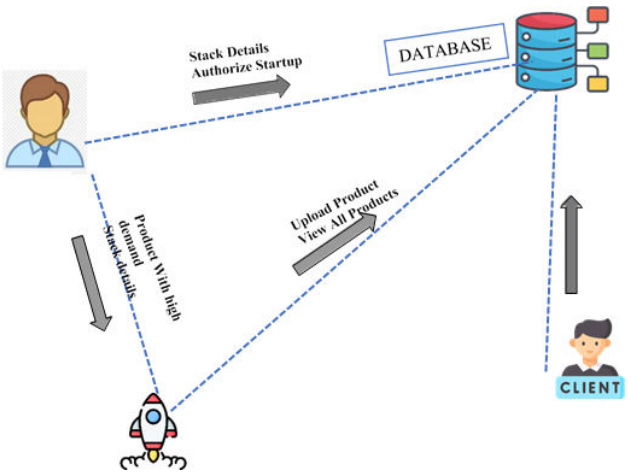


Fig. SYSTEM ARCHITECTURE

IV. IMPLEMENTATION

MODULES

- SENDER
- RECEIVER
- ADMIN
- CLOUD

MODULE DESCRIPTION

SENDER

Here sender is a module, sender should register to the application then only he can able to login into the application. After successful registration he must authorized by admin then only he can able to login into his account after login he can perform some operations such as can view his profile,

Here the sender can send the message in the form of DNA EncodeStep1: select receiver and write message Step2: convert original message to ascii code Step3: convert ascii to hexadecimal

Step4: convert hexadecimal to binary.

RECEIVER

Here receiver is a module, receiver should register to the application then only he can able to login into the application. After successful registration he must authorized by admin then only he can able to login into his account after login he can perform some operations such as can view his profile,

Here the receiver can decode the encoded DNA

Step1: verify decode key

Step2: convert DNA to binary

Step3: convert binary to hexadecimalStep3: convert hexadecimal to Ascii

Step4: convert ascii to original

.

ADMIN

Here admin is a module can able to login directly with the application, after successful login he can perform some operations such as view all senders and authorized them, view all receivers and authorize them and logout.

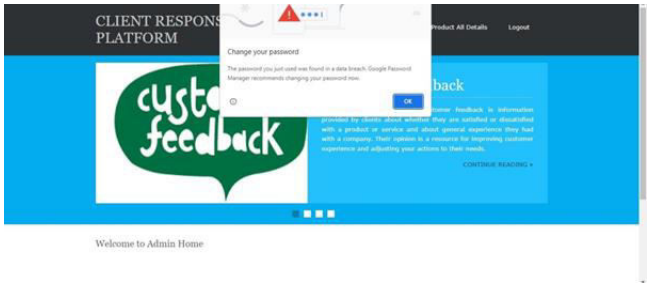
CLOUD

Here cloud is a module should login directly with the application after successful login he can perform some operations such as view original to ascii, view ascii to hexadecimal, view hexadecimal to binary, view binaty to DNA and logout.

V. SCREENSHOTS:

Home Screen

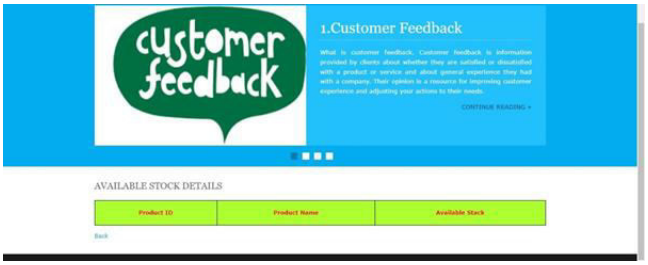
Login Screen



Admin Login

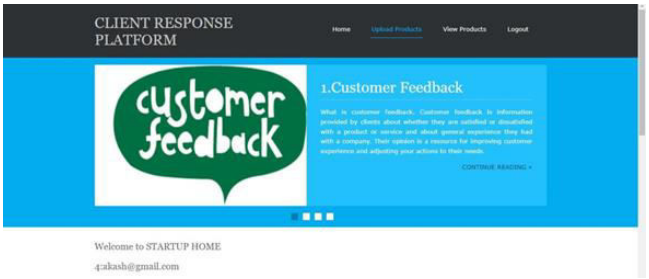
Registration Page

Available Stock Details

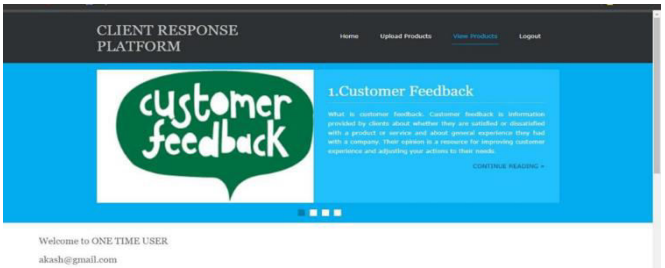


Purchased Products

Update Products



View Details



One time user

VI. CONCLUSION

Safeguarding user information in contextual social networks involves implementing a comprehensive approach to ensure privacy, security, and responsible data handling within the unique context of these networks. Here's a conclusion summarizing the key aspects of safeguarding user information in contextual social networks:

1. Data Encryption and Access Control:
Implement strong encryption techniques to protect user data both in transit and at rest. Utilizerobust access control mechanisms to limit access to sensitive information, ensuring that only authorized individuals can view or manipulate the data.

2. Privacy by Design:
Integrate privacy considerations into the design and development of the platform. This includes minimizing the collection of personal data, providing users with clear and transparent privacy policies, and obtaining explicit consent for data processing.

3. Anonymization and Pseudonymization:
Apply anonymization and pseudonymization techniques to dissociate personal information from specific individuals, reducing the risk of data breaches and unauthorized access while still allowing for valuable analytics and insights.

4. Regular Security Audits and Penetration Testing:
Conduct regular security audits and penetration testing to identify vulnerabilities and weaknesses in the system. Address any identified issues promptly to maintain a secure environment for user data.

5. User Education and Awareness:
Educate users about best practices for safeguarding their own information, such as setting strong passwords, being cautious about sharing personal data, and understanding the platform's privacy features. Encourage users to report any suspicious activities promptly.

6. Compliance with Regulations:
Adhere to relevant data protection and privacy regulations, such as GDPR, CCPA, or other regional laws. Ensure the platform's policies and practices align with the legal requirements to protect user rights and privacy.

7. Regular Data Purging and Retention Policies:
Enforce data retention policies to delete unnecessary user data after a specified period. This helps reduce the potential harm in case of a security breach and ensures that data is only stored for as long as necessary.

9. Continuous Monitoring and Alerts:
Implement continuous monitoring of the network and user data, utilizing intrusion detection systems and automated alerts to detect and respond to any unusual activities or potential security threats in real-time.

In conclusion, safeguarding user information in contextual social networks necessitates a holistic approach involving technological, regulatory, and educational measures. Striking a balance between providing valuable services and protecting user privacy is essential for building trust and ensuring the long-term sustainability of these networks.

In this paper, we proposed a new solution for privacy-preserving user profile matching with homomorphic encryption technique and multiple servers. Our solution allows a user to find out the matching users with the help of multiple servers without revealing the query and the user profiles. Security analyses have shown that the new protocol achieves user profile privacy and

user query privacy.

FUTURE SCOPE

Safeguarding user information in contextual social networks is a critical concern given the increasing amount of personal data shared and the potential privacy risks associated with it. Here are some future-focused strategies and considerations for enhancing user information protection in contextual social networks:

1. Privacy by Design and Default:
- Implementing privacy features into the design

and architecture of social networks from the outset. Privacy should be the default setting, and users should have granular control over their data sharing preferences.

2. Advanced Encryption and Security Measures:

- Enhancing encryption protocols and adopting state-of-the-art security measures to protect user data both during storage and transmission within the social network platform.

3. Decentralized Identity and Authentication:

- Implementing decentralized identity systems, like blockchain-based solutions, to allow users to control and manage their identity and personal data independently from the social network, enhancing privacy and security.

4. Collaboration and Information Sharing:

- Encouraging collaboration and sharing of best practices within the industry to collectively work towards developing more secure and privacy-focused solutions for contextual social networks.

The future of safeguarding user information in contextual social networks will involve a multidimensional approach, incorporating technology advancements, regulatory compliance, user empowerment, and a commitment to respecting individual privacy. Balancing the benefits of data sharing with the imperative to protect user privacy will be a central challenge in the evolving landscape of social networking.

REFERENCES

1. R. Agrawal, A. Evfimievski, and R. Srikant, Information sharing across private databases, in SIGMOD 2003, pp. 86-97.
2. M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, Veneta: Serverless friend-of-friend detection in mobile social networking, in IEEE WIMOB 2008, pp. 184-189.
3. B. H. Bloom, Space/time trade-offs in hash coding with allowable errors, Communications of the ACM 13 (7): 422-426, 1970.
4. D. Boneh, E. J. Goh, K. Nissim, Evaluating 2-DNF formulas on ciphertexts, in TCC 2006, pp 325-341.
5. D. Chaum, Blind signatures for untraceable payments, in Crypto 1982, pp. 199-203.
6. E. D. Cristofaro and G. Tsudik, Practical private set intersection protocols with linear complexity, in Financial Cryptography and Data Security 2010.
7. D. Dachman-Soled, T. Malkin, M. Raykova, and M. Yung, Efficient robust private set intersection, in ACNS 2009, pp. 125-142.
8. T. ElGamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (4): 469-472, 1985.
9. M. Freedman, K. Nissim, and B. Pinkas, Efficient private matching and set intersection, in EUROCRYPT 2004, pp. 1-19.
10. C. Gentry, Fully homomorphic encryption using ideal lattices, in STOC 2009, pp 169-178.
11. Zhe Liu, Le Yu, Wenbo He, "Privacy and Security in Online Social Networks: A Survey" Published in: IEEE Communications Surveys & Tutorials, 2015
12. Joseph Bonneau, Sören Preibusch, "A Survey of Privacy in Online Social Networks" Published in: ACM Computing Surveys, 2010
13. S. Guha, Ravi Kumar, D. Rajan, Andrew Tomkins, "Preserving Privacy in Social Networks" Published in: ACM SIGMOD Record, 2008
14. David Salomon, "User Data Privacy: Facebook, Cambridge Analytica, and the EU General Data Protection Regulation" Published in: IEEE Security & Privacy, 2018
15. Mohamed Medhat Gaber, Ajith Abraham, "Data Privacy in Social Networks: A Survey" Published in: Data Mining and Knowledge Discovery, 2010
16. Wenjia Li, Lingling Xu, et al. , "Privacy-Preserving Location-Based Services for Mobile Users in Cloud Computing" Published in: IEEE Transactions on Emerging Topics in Computing, 2015
17. Petra M. Mäntylä, Tarmo Toikkanen, "Building Online Communities in Higher Education Institutions: Creating Collaborative Experience" Published in: Springer, 2018
18. Shouling Ji, et al., "Securing the Privacy of Sensitive User Profile Attributes in Social Networks" Published in: IEEE Transactions on Information Forensics and Security, 2013.