Research Article

Enhancing Security And Privacy For E-Commerce Database

kanakanti balakrishna reddy[1], Subramanian[2]
[1]Research scholar,, Saveetha Institute of medical and technical sciences, Chennai, T.M, India balakrishnareddy1998@gmail.com ,
[2]Assistant professor, Saveetha Institute of medical and technical sciences, Chennai, T.M, India eksdeal@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

ASTRACT: The cloud computing are the services offered in the Internet and everyone using the cloud services and more over every android user using the database. All users are having some confidential information. Proposed system provides security for the information in databases by implementing the one of the best algorithms and these algorithms may provide more security. Unauthorized people may access confidential information without any permission. The popular security algorithms are AES (Advanced encryption standard), DES (Data encryption standard, CES (cipher block standard ,3DES, RSA. These algorithms we have encrypt the data and decrypt them to protect from the attack or any Phishing attacks or any vulnerability to keep our information safe. But the attackers can break present technologies and access the information. In this kind of scenario, at least sensitive private information should not be disclosed. Hence the proposed system concentrates on the privacy of an information and considers the biometric security.

Keywords: cloud computing, algorithms, information, security, biometric.

INTRODUCTION:

Cyber-attacks and security loopholes and the vulnerabilities are also improved. Now a days every common user or every people are using the banking system through entire e-commerce web site, booking online tickets. They trust and give the entire information. Because they trust the web sites, if in case data loss or attack, we cannot recover data, that is the reason why we are using the cloud services to improve the space and storage and security by encryption and decryption of the data and this approach is proposed in this article.

[1] Cloud computing is the one of the best storage systems on demand in present situation why because the accessing data in cloud is anywhere and everywhere.

Different services like software as service, platform as service, infrastructure as services, public, private, hybrid are the different types of the services available on cloud.

Security provided commonly using the (AES) algorithm. Proposed system is using the (RSA) Rivest, Shamir, adleman. This algorithm is mainly using the encrypted and decrypted process. This algorithm is mainly using the secure, sharing our any of information. whenever transferring our data, virus may also attacking, then we cannot do anything that’s why have to mainly concentrate security problems. **A.Distributed Denial of services (DDoS**) – Quality of services are degraded or services are unavailable due to failures of multiple infrastructure and network resources. This will lead to unavailability of systems to customers to carry out financial transaction and working staff to perform their operational duties effectively. This will in turn disrupt the normal flow of life and affect economy as a whole. In case of DDoS, the attack may not be detectable as the sources of attack may be from various locations and virtual. This will increase the recovery time required for systems to return to normal business activities. **b. Corruption (Tampering) of programs and / or data – Programs** and / or data are modified in unauthorised way. Depending upon the type of program corrupted (financial processing, customer data, storage systems, connectivity devices etc.); the impact will be either financial or operational loss or both. In banking and financial services is industry to, a small introduction.

Phishing: Through phishing, a customer of the bank may be prompted to enter credentials of the account which can be stored in system and used in future to carry out financial transaction. Due to phishing, bank’s customer may lose personal information and financial wealth which will look like authentic for both customer & bank and will go undetected.

SMS Spoofing: Through SMS spoofing a user receives a SMS from unknown source asking to provide account details and credentials in order prevent theft or risk of loss of money; through this customer details can be captured during the process and can be used later to steal money from account. TCP/IP spoofing: In this type of vulnerability, an email is sent to user (bank’s customer) that appears from the genuine source, this technique is powerful as it bypasses the firewall as IP address looks to be external. This method gives access to financial system (server) to external parties which can damage the system as a whole or steal information.

Privilege escalation: Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. For example, a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full unrestricted access to a system.

Vishing: Vishing is use of voice and phishing, in which a person pretends to be calling from bank or financial institution in order to access private and financial information from the public .Once, the person gives details (Account number, card information etc.), they are used to perform financial transaction (theft) from bank account which looks genuine and by the person, which leads to financial loss for person. This act can also be termed as Social Engineering.

Cross site scripting (XSS): XSS is the method to include malicious codes in webpages visited by the user. The data entered by user are later used to create fake identifies, open accounts and perform financial transaction which will cause financial losses to actual customer or person.

[1] Google Assistant is used and secure our entire of data that is the mainly implemented in the online banking system by using the cloud storage and considered as one of the best feature used here.

PROPOSED METHODOLOGY:

The proposed system implemented methodology using (RSA) algorithm and Google assistant.

The software and tools that are used in this proposed system are Matlab , data base ,net beans. Since the storage service is available in cloud, the data is stored in cloud. To upload the documents in cloud, have to provide finger print and security pin and these are best implemented.

Note : RSA algorithm pseudocode

```
def gcd(a,b):
    if b==0:
        return a
    else:
        return gcd(b,a%b)
p = int(input('Enter the value of p = '))
q = int(input('Enter the value of q = '))
no = int(input('Enter the value of text = '))
n = p*q
t = (p-1)*(q-1)


for e in range(2,t):
    if gcd(e,t)== 1:
        break
for i in range(1,10):
    x = 1 + i*t
    if x % e == 0:
            d = int(x/e)

            break

ctt = Decimal(0)

ctt =pow(no,e)

ct = ctt % n


dtt = Decimal(0)

dtt = pow(ct,d)

dt = dtt % n

print('n = '+str(n)+' e = '+str(e)+' t = '+str(t)+' d = '+str(d)+' cipher text = '+str(ct)+' decrypted text = '+str(dt))
```

Screenshots:

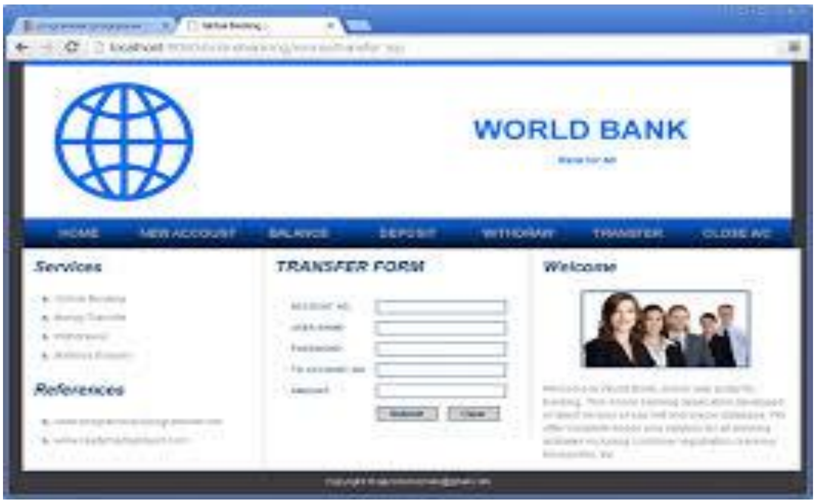

Fig.1 Login page

Fig.2 Finger print security

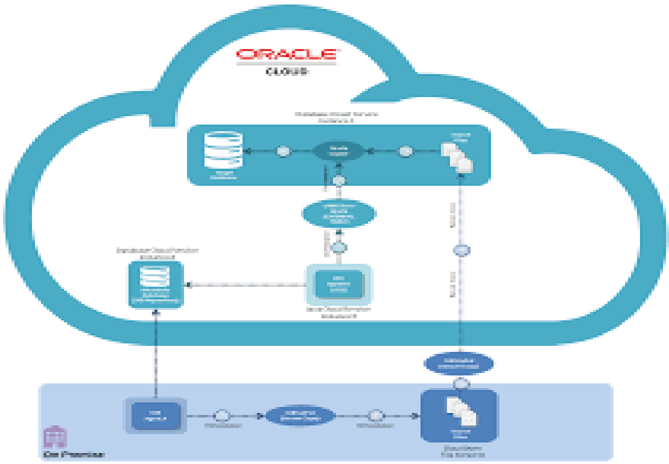

Fig.3 Cloud data upload

FUTURE SCOPE:

BANKING ON THE CLOUD : However, The cloud offers a host of opportunities for banks to build a more flexible and customer-centric business model that can drive profitable growth and, as a result, should be something that non-IT decision makers at bank understand and appreciate. So what does the future of cloud computing look like for banks—both in the near and long term? The pundits tend to overestimate the impact of a technology and paradigm shift in the short term and underestimate what happens in the long term. In this paper, we explore some forward thinking that uses cloud computing in the banking sector and discuss ways we believe innovative banks will be leveraging the cloud for competitive advantage in the next five years. Cloud computing is one of the hottest technology and business topics today, and the market for cloud services is expected to skyrocket in the next few years. Cloud computing can help financial institutions improve performance in a number of ways. A. Cost Savings and Usage-based Billing With cloud computing, financial institutions can turn a large up-front capital expenditure into a smaller, ongoing operational cost. There is no need for heavy investments in new hardware and software. In addition, the unique nature of cloud computing allows financial institutions to pick and choose the services required on a pay as-you-go basis. B. Business Continuity With cloud computing, the provider is responsible for managing the technology. Financial firms can gain a higher level of data protection, fault tolerance, and disaster recovery. Cloud computing also provides a high level of redundancy and back-up at lower price than traditional managed solutions. C.Business Agility and Focus Cloud computing also allows new product development to move forward without capital investment. Cloud computing also allows businesses to move non-critical services to the cloud, including software patches, maintenance, and other computing issues. As a result, firms can focus more on the business of financial services, not IT. The flexibility of cloud-based operating models lets financial institutions experience shorter development cycles for new products. This supports a faster and more efficient response to the needs of banking customers. Since the cloud is available on-demand, less infrastructure investments are required, saving initial set-up time.

CONCLUSION

Banking system is improved with confidential information sharing everywhere and protection from attack also improved. To use debit cards to pay any of the   products purchase, there must be a trust between business entity and cloud users to make the e-banking system a success one. Privacy and security are the emerging issues in E-commerce. The paper discusses the privacy issues in E-commerce and provides a guideline to facilitate the users in doing the online transaction in a safe and secured mode. Currently, privacy is considered as a public issue, a proper mechanism is needed for the enforcement of data privacy in E-commerce. We mention some important precaution and security step that ensure that the user’s privacy is not at risk.

References:

1. Budak C, Goel S, Rao J, Zervas G (2016) Understanding emerging threats to online advertising. ACM Conference on Economics and Computation pp: 561-578.
2. Lee I (2016) User Privacy Concerns for E-Commerce. IGI Global:Encyclopedia of E-Commerce Development, Implementation, and Management pp: 1780-1787.

3. Ackerman MS (2004) Privacy in pervasive environments: next generation labeling protocols. Personal and Ubiquitous Computing 8: 430-439.4.Ackerman MS, Davis TD (2003) Privacy and security issues in e-commerce. New economy handbook pp: 911-930.
4. Smith R, Shao J (2007) Privacy and e-commerce: a consumer-centric perspective. Electronic Commerce Research 7: 89-116.
5. Corbitt BJ, Thanasankit T, Yi H (2003) Trust and e-commerce: a study of consumer perceptions. Electronic commerce research and applications 2: 203-215.
6. Lau RY (2007) Towards a web services and intelligent agents-based negotiation system for B2B eCommerce. Electronic Commerce Research and Applications 6: 260-273.
7. Castañeda JA, Montoso FJ, Luque T (2007) The dimensionality of customer privacy concern on the internet. Online Information Review 31: 420-439.
8. Kritzinger E, Smith E (2008) Information security management: An information security retrieval and awareness model for industry. Computers & Security 27: 224-231.

https://www.researchgate.net/publication/276492996_Influences_of_Cloud_Computing_on_E-Commerce_Businesses_and_Industry

https://www.scirp.org/(S(i43dyn45teexjx455qlt3d2q))/reference/ReferencesPapers.aspx?ReferenceID=1091050

http://pub.benjaminblau.de/Business_Models_in_the_Service_World.pdf

https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=1091044

https://www.semanticscholar.org/paper/A-Systematic-Review-on-Cloud-Computing-Singh/db2cef23a2abb52249241a65032f55226cbafbe7

https://www.ijcaonline.org/archives/volume88/number6/15356-3817

http://www.ijptonline.com/wp-content/uploads/2017/02/23690-23701.pdf

http://pub.benjaminblau.de/Business_Models_in_the_Service_World.pdf

https://www.researchgate.net/publication/224178604_The_management_of_security_in_Cloud_computing

https://www.scirp.org/(S(351jmbntvnsjt1aadkposzje))/reference/ReferencesPapers.aspx?ReferenceID=839324

https://link.springer.com/chapter/10.1007%2F978-3-642-30223-7_3