A secure authentication and data security for online banking in cloud environment

Ranjana Singh, AS.prof Kite Patil, AS.Prof Ashish Tiwari

Software System,Vindhya Institute of Technology & science
Umarikheda,Khandwa Road,Indore,Madhya Pradesh 452020

***Abstract*—**Among a number of internet based applications the internet banking is a most popular application now in these days. A rich number of users are directly connected for 24 hour digital banking. Due to this the traffic load on the banking servers are increases significantly therefore a scalable computing solution is required for banking. On the other hand for designing the banking system there are two primary security aspects are required to follow first the secure authentication and the secure data transmission between client and server. Therefore in this presented work the investigation about the banking security and their authentication process is performed. In addition of that for scalable services the proposed model is deployed using the openshift cloud environment.The proposed banking solution contributes in both the domain of security namely authentication and network data security. To achieve the improved solution for authentication the client server mutual authentication process is followed. In this technique client verifies the server through the image and text associated. And the server verifies the client using the random question answering. Additionally for more secure environment the OTP is also used for authentication. On the other hand for securing the communication among the client and server communication a hybrid cryptographic solution is presented. The cryptographic solution is developed with the help of MD5 hash generation algorithm and the ECDH secure encryption technique.The implementation of the proposed banking solution is provided using the JAVA technology. Additionally the deployment of the solution is provided in the OpenShift cloud platform. Moreover for investigating the cryptographic overhead during the communication the proposed cryptographic solution is compared with the RSA algorithm. The experimental results show the proposed technique consumes less amount of time for encryption and decryption as compared to the RSA algorithm. Additionally also consumes less memory for the computational aspects.

***Keywords*—** online banking, cryptography, authentication, data security, network security

I. INTRODUCTION

Now in these days the popularity of the internet and internet based applications are increases continuously. Additionally a significant amount of new users are also involving for finding the data and services on the internet. Therefore the traditional computing technology are not provides the efficient services for new generation computing needs. The new technology namely cloud computing is providing a new way of computation. That offers scalable computing and also offers the scalable storage for huge amount of request processing. Thus in this presented work the banking solution is prepared for the cloud computing domain. The cloud computing can able to handle a large volume of the user's request and also provide the efficient manner and response from the server.

On the other hand the banking applications need the security and privacy due to the commercial information is a kind of sensitive information. And security lack can harm the bank and customers also. Therefore there are two different aspects of security is required.

1. **During the communication between the user and server:** the communication among the client and server is always performed in unsecured infrastructure. Because the client and server systems are secured with some kinds of firewalls and anti-virus techniques but the public network which is used during the communication is not much secured due to various kinds of attacks i.e. man in middle attack.
2. **During the authentication of online banking system:** the secure online banking need a secure authentication technique also because the various kinds of attackers can also tries to break the online security and tries to make some frauds.

Therefore the proposed solution is required to provide the solution for all the discussed domains of security, authentication and server response. This section provides the overview of the proposed study domain. In the next section the proposed methodology for security system design is presented.

II. PROPOSED WORK

The proposed technique of the security implementation on the cloud based online banking is demonstrated using the figure 1.

ISSN: 2278 – 1323

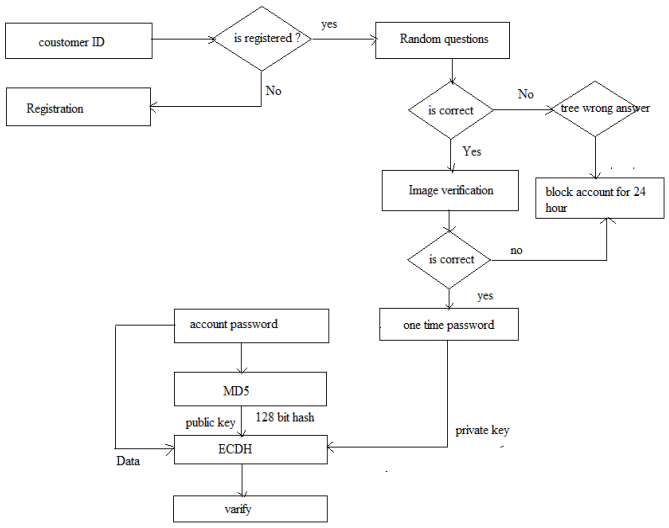

Figure 1 proposed methodology

The entire system can be divided into two major domains first the authentication process and second the cryptographic data exchange during the communication.

Authentication process

The given initiate their working when the user provides input their customer id. If the given user is registered with the banking solution then the system precedes further for authentication otherwise the system return the error for user. Therefore the user is not registered with the system and need to perform the registration with the system.

For authentication first user provides their customer id to the system and system recognize the user. After that a security question is asked by system to the user. During the registration process these questions and their answers are stored on the database. Therefore during the authentication a random question from the previous one is asked to the user. If the user answers three time false answer then the account is blocked for 24 hours. In the same ways the image security is implemented. These images are selected by the end user during the registration additionally the associated tags are also provided by the user. If the user identify their provided image then the tag input is required correctly. If the answer is appropriate then then for finalization of the authentication process system send an OTP to the end user. After that the user can access the entire utilities of the system.

Cryptographic data exchange

The proposed cryptographic solution is a hybrid cryptographic activity, that is usage two different methods one usage the MD5 algorithm and then the encryption and decryption is performed at the server end using the ECDH algorithm. The entire process of the proposed cryptographic solution is given as:

Input: Account password P_a, OTP O, Data communicated D_c Output: cipher for communication C_d
Process: 1. O = Extract_Recent_OTP() 2. K= generate_Hash_MD5(P_a) 3. C_d = ECDH_encrypt(D_c, K, O) 4. Return C_d

Table 1 cryptographic data exchange

III. RESULTS ANALYSIS

The implementation of the secure authentication technique for banking application is successfully completed. After the implementation the performance of the system is different performance parameters are evaluated and reported in this chapter.

A. Encryption time

The amount of time required to encrypt the data is termed as the encryption time. In this presented work encryption time is evaluated in terms of milliseconds.

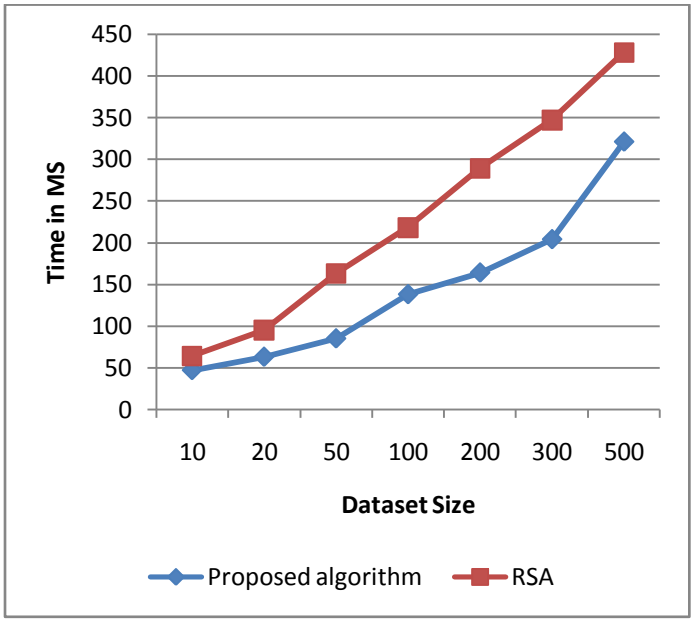

Figure 2 encryption time

The given figure 2 shows the comparative performance in terms of RSA traditional encryption algorithm and the proposed hybrid algorithm in terms of encryption time. In order to shows the performance of both the algorithm the blue line shows the performance of the proposed algorithm and the traditional algorithm is demonstrated using the red line. In this diagram the X axis shows the different experiments performed with the system and Y axis shows the performance of the algorithms in terms of milliseconds. According to the

ISSN: 2278 – 1323

comparative performance analysis the proposed algorithm encrypt the data more efficiently and in less time consumption as compared to the traditional RSA algorithm.

B. Decryption time

The amount of time required to recover the original text from the input cipher text is termed as the decryption time. The decryption time of both the algorithms namely proposed and RSA

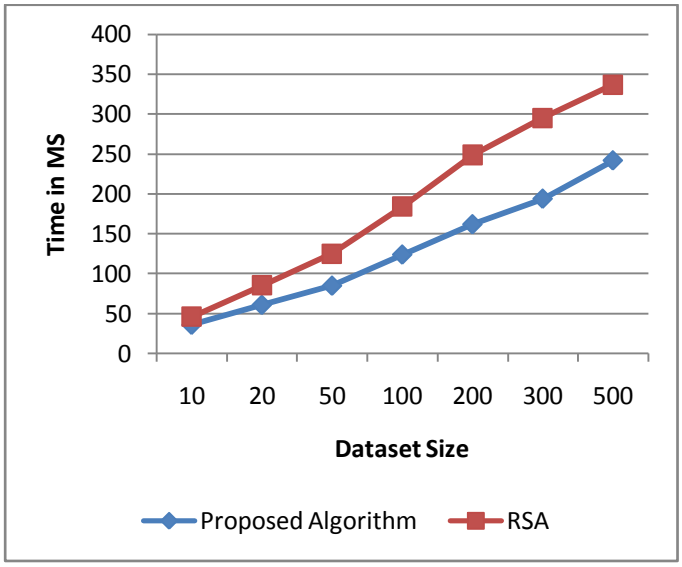

Figure 3 decryption time

The figure 3 shows the performance of both the implemented algorithms, the performance of the proposed algorithm is given using blue line and the red line shows the performance of the RSA algorithm. In order to demonstrate the performance of the system the X axis contains the different experimental set of dataset size and the Y axis shows the performance in terms of milliseconds. According to the obtained performance of the system the proposed algorithm consumes less amount of time as compared to the RSA algorithm. Thus the proposed algorithm is much adoptable as compared to the traditional cryptographic algorithm.

C. Memory consumption

The amount of main memory required to execute the algorithm is known as the memory consumption of the system. The given figure 4 shows the comparative memory consumption of both the algorithms. In this diagram the amount of memory consumes is given in Y axis and the different experimental sets are given using the X axis. According to the obtained results the memory consumption is similar to the amount of data stored in the main memory. As the results shows the performance of RSA and proposed cryptographic algorithm, the performance of the proposed algorithm is much effective than the traditional algorithm RSA.

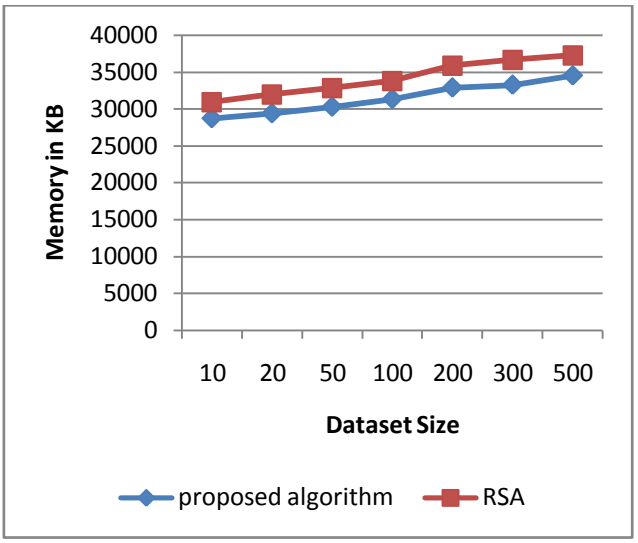

Figure 4 memory consumption

IV. Conclusions

The given section provides the summary of the entire proposed work and their implementation. Additionally based on the observations and experiments of the proposed system some facts are concluded which are also provided in this chapter. Finally for the future extension of the proposed work some suggestions are also made which is also reported.

A. Conclusion

The need of computation leads to invent new technology for satisfying the current needs. Therefore the new generation need of internet usages are increases continuously and for supporting these needs the traditional computing is turned into the cloud computing. The cloud computing offers scalable computing, storage and trust worthy computing. Therefore using the cloud computing a new solution for new generation banking is proposed. In addition of that for formulating the solution of the current banking issues and online banking frauds two major issues are targeted. First need to improvement on the current online banking authentication policies for phasing and similar kinds of attack prevention. Additionally the secure communication among the client and server is also proposed suing the cryptographic data exchange.

Therefore a client server mutual authentication based approach is proposed for authentication and for securing the communication the hybrid cryptographic solution is proposed. The authentication scheme involves the random image based user verification, random question based verification and during transections the OTP is used. Additionally when the data is communicated between user machine and the banking application server the cryptographic solution is implemented. That cryptographic technique is efficient, secure and light weight due to use of ECDH algorithm with the MD5 algorithm. The MD5 algorithm is first use to generate the hash key for encryption and then using the ECDH the entire cryptographic process is taken place.

ISSN: 2278 – 1323

The implementation of the proposed security system is provided using the JAVA technology. Additionally for deployment the open cloud (public cloud) i.e. openshift is used. The proposed method is evaluated with respect to RSA algorithm which is one of the security or cryptographic technique utilized. The evaluated comparative performance of both the cryptographic systems is given using the table 2.

S. No.	Parameters	Proposed	RSA
1	Memory consumption	Low	High
2	Encryption time	Low	High
3	Decryption time	Low	High

Table 2 performance summary

The proposed system is able to provide the solution for both the aspects of security and privacy. Therefore that is adoptable for the secure banking and the authentication.

B. Future work

The proposed cloud based secure online banking model is adoptable for their efficiency and security. Therefore the future extensions of the proposed system are feasible for the following directions.

1. The proposed work is not tested on the real world test beds therefore need to evaluate the real world constrains before extending the proposed security model.
2. The proposed model is implemented with the MD5 algorithm for improving the performance of cryptographic data exchange. Thus for improving security SHA algorithm can also be used with the system.

REFERENCES

[1] Milton Kazmeyer, "Security Issues Relating to Internet Banking", http://yourbusiness.azcentral.com/security-issues-relating-internet-banking-21683.html
[2] Ming Li, Shucheng Yu, Yao Zheng, KuiRen, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013
[3] torryharris, "CLOUD COMPUTING – An Overview", http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf
[4] Vaishali Jain, Akshita Sharma, "A Taxonomy on Cloud Computing", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 3, March 2014
[5] Balvinder Singh, Priya Nain, "Bottleneck Occurrence in Cloud Computing", National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012)
[6] KratiMehto, Rahul Moriwal, "A Secured and Searchable Encryption Algorithm for Cloud Storage", International Journal of Computer Applications (0975 – 8887) Volume 120 – No.5, June 2015
[7] PradipLamsal, "Understanding Trust and Security", Department of Computer Science University of Helsinki, Finland, 20th of October 2001
[8] RajnishNoonia, ".Net Cryptography (Encryption / Decryption)", http://www.pixytech.com/rajnish/2013/04/net-cryptography-encryption-decryption/
[9] A. SHARMA and S.K. LENKA, "Analysis of QKD multifactor authentication in online banking systems", BULLETIN OF THE POLISH ACADEMY OF SCIENCES TECHNICAL SCIENCES, Vol. 63, No. 2, 2015
[10] SonawaneShamal, Khandave Monika, NemadeNeha, "Secure Authentication for Online Banking Using QR Code", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 3, March 2014
[11] O.B. Lawal, A. Ibitola, O.B. Longe, "Internet Banking Authentication Methods in Nigeria Commercial Banks", African Journal of Computing & ICT, Vol 6. No. 1, March 2013
[12] Khalid Waleed Hussein, Nor FazlidaMohd. Sani, RamlanMahmod, Mohd. Taufik Abdullah, "Active Authentication by one Time Password Based on Unique Factor and Behavioral Biometric", International Journal of Computer Networks and Security, ISSN: 2051-6878, Vol.23, Issue.2
[13] K.Thamizhchelvy, G.Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm", 2012 International Conference on Computing Sciences, 978-0-7695-4817-3/12 $26.00 © 2012 IEEE
[14] Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, Ahmad-Reza Sadeghi, "On the (In)Security of Mobile Two-Factor Authentication", TechnischeUniversit¨at Darmstadt Center for Advanced Security Research Darmstadt D-64293 Darmstadt, Germany, First Revision: January 31, 2014
[15] SaurabhPanjwani, "Practical Receipt Authentication for Branchless Banking", DEV '13, January 11-12, 2013 Bangalore India Copyright c 2013 ACM
[16] A.SaiSuneel, S.B.Sridevi, K.Nalini, "Dual Security Using Fingerprint and Password in Banking System", International Journal of Review in Electronics & Communication Engineering (IJRECE) Volume 1 - Issue 3 August 2013
[17] Ali Abdollahi, Mehdi Afzali, "A SINGLE SIGN-ON BASED INTEGRATED MODEL FOR E-BANKING SERVICES THROUGH CLOUD COMPUTING", International Journal of Advances in Computer Science and Technology, Volume 3, No.1, January 2014
[18] Anand Sharma, S.K.Lenka, "Authentication in Online Banking Systems: Quantum Cryptography Perspective", International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014

.

ISSN: 2278 – 1323