IJRRECS/August 2014/Volume-2/Issue-8/2908-2912 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

PROVISION OF AUTHENTICATED COMMUNICATION BY QUANTUM SYSTEM

Kunchala Vijayanarasimha Reddy[1], Thirupathi Reddy Thumma[2]

[1]M.Tech Student, Dept of CSE, Aurora's Scientific And Technological Institute, Aushapur(V), Ghatkesar(M), R.R Dist, T.S, India

[2]Associate Professor, Dept of CSE, Aurora's Scientific And Technological Institute, Aushapur(V), Ghatkesar(M), R.R Dist, T.S, India

ABSTRACT:

Here a new technique is proposed for the purpose of the distribution of the data n a well efficient manner followed by the scenario of the well efficient technique of the protocol related to the scenario of the third party based authentication is taken into the consideration under the key distribution of the data authentication under the environment of the third party is a primary concern. It is completely different and well advanced compared to that of the several previous methods in a well acquainted fashion under the security based aspect is a major concern. Here the system is completely independent of the computational complexity in a well effective manner rather compared to that of the standardized data key based encryption is a major concern in its implication as per the medium of the transmission under the properties of the physical environment according to the standards of the properties of the mechanics of the quantum plays a crucial role respectively. Here the sharing of the data related to the information under the scenario of the concealed participants of the trust oriented with respect to the third party as per the scenario of the authentication respectively. Here the implementation o ff the present method is designed in a well accurate manner under the system well oriented in terms of the network based architecture of the sensitive data used under the network oriented constraints under the institutional basis respectively. Simulations have been conducted on the present method a huge

amount of analysis takes place on the large number of the test bed in a well oriented fashion for the verification of the outcome of the entire system in terms of the performance analysis or evaluation respectively.

KEYWORDS: Data encryption standard, Data authentication, Protocol under distribution, Quantum authentication, Cryptography, Information based on the sensitive strategy, Information of patient and computation of cloud respectively.

1. INTRODUCTION:

Nowadays security is a major concern and plays a crucial role for the development of the system in terms of the implications of the trust based user is a major concern. Here we get popularity only by satisfying the customers based on the functioning of the module or the software services depending on their own requirements is a major concern [1]. There are lot of techniques implemented earlier and some of them includes the standards of the advanced encryption followed by the structural representation of the basis of the RASA respectively. Here there are lot of the classical previous methods and they are facing a large number of the drawbacks in a well efficient manner. So therefore there is a necessity of the rapid advancement needs to be done in the system for the getting importance apart from the user and based on the this scenario the performance of the system is evaluated based on the structural representation respectively [2][3]. Therefore there is a necessity of the requirement of the development of the new advanced tehnique for the well effective analysis of the system in an oriented fashion respectively. Here the system is mainly facing the challenge of the advanced encryption standards apart from the advancement of the data encryption schemes on the basis of the data security and the privacy of the data is a major concern. Apart from that many of the schemes are implemented on the basis of the cryptography as one of the data security and protection is a major concern respectively [4][5].

BLOCK DIAGRAM

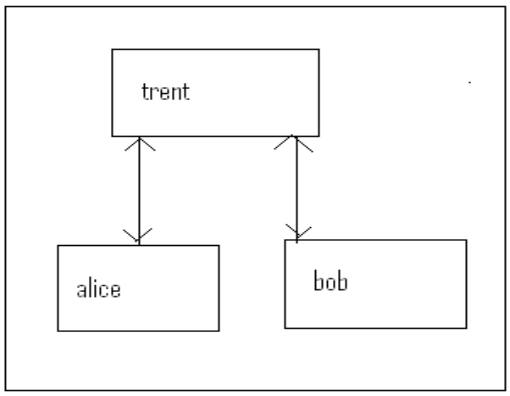

Fig 1: Shows the block diagram of the present method respectively

2. METHODOLOGY:

In this paper a new technique is presented where ti completely overcome the drawbacks of the several previous methods in a well oriented fashion respectively [7][8]. Here the implementation of the present method is shown by the above block diagram and is explained in the summarized fashion respectively. Here there is an implementation of the scheme based on the advanced phenomena relative to the strategy of the distribution of the key based on the quantum authentication is a primary concern [9]. Here for the improvement or the development of the system a protocol is designed in a well suitable fashion by the help of the QAKD and its analysis point of view followed by the well effective integration of the servers oriented with the third party is a major concern respectively [10]. Therefore as in the previous methods there the algorithms are design in the basis on the monotonic strategy that is either of the one is selected and then implemented in a well effective manner and here the integration of the couple of the methods in a together fashion for the well effective analysis of the system and the improvement in the performance plays a major concern respectively.

3. EXPECTED RESULTS:

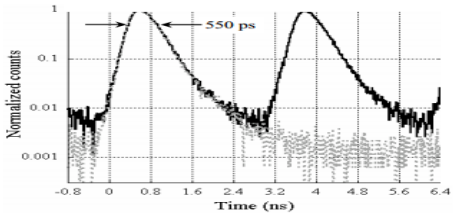

Fig 2: Shows the graphical representation of the present method respectively

The evaluation of the performance of the system takes place by the help of the graphical representation where the comparative analysis is made by a systematic approach in which the evolution of the performance of the system takes place in a well oriented fashion respectively. Here the present method studies the in depth

analysis of the several previous methods and its problems followed by the challenges faced by it in order to improve the performance of the present system and also the scenario of the conducting of the large number of the test beds in a well acquainted fashion respectively. Here an algorithm is used that is designed by the help of the encryption standard followed by the process of the decryption at the time of the retrieval of the data depending on the necessity of the user and it is related to the scenario of the algorithm of the effective functioning of the system based on the encryption standard of the commutative scenario respectively. Here the analysis of the present method takes place by the proper analysis of the data that is implemented in a sequential scenario in which there should be no loss of data that is protected completely from the effects associated with it and also the trust is also gets satisfied by the above security algorithm for the user. Here we finally conclude that the present method is effective and efficient in terms of the performance followed by the outcome of the entire system in a well oriented fashion respectively.

4. CONCLUSION:

In this paper a new technique is presented for overcome the huge challenges faced by the several previous techniques in a well efficient fashion n terms of the data encryption where the privacy of the user or the customer is a major concern in terms of building the popularity among the users. There are a lot of technique as previously developed by the system but many of them are facing the problems in terms of the security based aspect followed by the attacks prone is a serious problem respectively. Here in the implementation of the present method is designed by the help of the new protocol which is having a well effective mechanism under the constraints of the key oriented authentication of the third party plays a crucial role which includes the participation of the distribution and also relative to the structural aspects of the information sharing and the proper maintenance of the of the trust of the user that is the privacy of the data related to the user is a major concern respectively. Here for the proper maintenance of the third party based authentication a new mechanism is designed under the well effective consideration of the third party is the mechanics of the quantum statistics is a

major concern. Here for the proper implementation of the design oriented strategy there is a mechanism under the prominent protocol of the TTP which includes the functionality of the constraints of the participants involved in it and the key of the session plays a major role under the environment of the institutions respectively. Here by the proper integration of the protocol of the TTP there is a provision of the security and the privacy problem is completed eliminated and the customer problem is reduced where by this there can be a popularity for the sake of the system and then the performance of the entire outcome of the system is evaluated. Here the protocol used in the system is under the constraints of the integrated fashion by which it includes the proper functionality of the third party based random sharing of the data related to the strategy of the sensitive institutions plays a crucial role.

REFERENCES

[1] Y. Kanamori, S.M. Yoo, and F. Sheldon, "Bank Transfer over Quantum Channel with Digital Checks," IEEE GlobeCom 2006, San Francisco, CA, Nov. 2006.

[2] Y. Kanamori, S.M. Yoo, D.A. Gregory, and F. Sheldon, "Authentication Protocols using Quantum Superposition States," to appear in International Journal of Network Security.

[3] J.W. Byun D.H. Lee and J.I. Lim, "Security analysis and improvement of a gateway-oriented password- based authenticated key exchange protocol," IEEE Communications Letters, Vol. 10, Issue 9, pp. 683 – 685, 2006.

[4] T. Cao and D. Lin, "Cryptanalysis of two password authenticated key exchange protocols based on RSA," IEEE Communications Letters, Vol10, Issue 8, pp. 623-625, 2006.

[5] W. Stallings, Cryptography and Network Security – Fourth Edition, Pearson Prentice Hall, NJ, 2006.

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. of Modern Physics, vol. 74, pp. 145-190, 2002.

[7] W.K. Wootters and W.H. Zurek, "A Single Quantum Cannot Be Cloned," Nature, vol. 299, pp. 802-803, 1992.

[8] D.J. Griffiths, Introduction to Quantum Mechanics, New Jersey, Prentice Hall, 1995.

[9] C. H. Bennett, F. Bessette, G. Brassard, L.Salvail, and J. Smolin, "Experimental quantum cryptography," Journal of Cryptology, vol. 5, no.1, 3 - 28, 1992.

[10] P. Kitsos and O. Koufopavlou, "Efficient architecture and hardware implementation of the Whirlpool hash function, " IEEE Transactions on Consumer Electronics, Vol 50, Issue 1, pp. 208 – 213, 2004.