International Journal of New Technology and Research (IJNTR)
ISSN:2454-4116, Volume-2, Issue-4, April 2016 Pages 144-147

Database Security of E-Commerce Based on Hybrid Encryption

Aditi Gupta

***Abstract*— E-business database is extremely helpful in today's reality as it continued creating and winning tremendous benefit. Information in a database in e-trade is vital. We should have the complete security. Information is the most important resource in today's reality as it takes day –to-day life structure as it record everyday exchange. Databases are the most loved focus to the aggressors. Despite the fact that the examination of client enrollment and recovering secret key, the security issue existing as the conventional strategy for recording in e-business. On the premise of symmetric and hilter kilter encryption advances the half breed encryption advances has been sent to consolidate both of the past advances. Mixture encryption innovation has been to enhance the database security of –ecommerce.**

***Index Terms*— E-Commerce, Database Security, Hybrid Encryption, Symmetric Encryption, Asymmetric Encryption**.

I. INTRODUCTION

Information is the most important resource in today's reality as it record everyday exchange "what comes in and what goes out". Security is the most essential subject in e-business. To secure the information we put away in the database. Database is gathering of information which stores various information in a solitary spot. In this way the security of database is must. Security is considered as a test these days.

One of the fundamental points come is that how to secure the data as indicated by budgetary organization we need to screen customer accounts, market plan and trade asset thus forth[1]. Right away at present we see that the advancement which has been used as a piece of e-exchange databases are according to the accompanying: "Web access control, user authentication, backup and recovery, data encryption" and so on. There is one innovation specifically encryption advancement which is to a great degree effective to ensure database security. The essential encryption development including symmetric and uneven encryption which won't give a fitting result and does not prompt securing database on system. So keeping in mind the end goal to take care of the issue we fundamentally utilize crossover encryption innovation as a blend of symmetric and topsy-turvy encryption innovation.[1]

II. SECURITY ISSUES

In an e-trade database sets fills in as an open situation. To guarantee the security of essential data is the initial phase in an e-commerce.[2] There is a stream outline that will clarify the client registration[13].

The most surely understood purpose behind database vulnerabilities is a nonappearance of due thought at this moment they are passed on. Though any given database is striven for handiness and to guarantee it is doing what the databases is planned to do, not a lot of checks are made to check the database is not doing things it should not be doing. Databases may be seen as a "back end" part of the work environment and secure from Internet-based risks (along these lines data doesn't should be mixed), be that as it may this is not the circumstance. Databases also contain a frameworks organization interface[9], in this way software engineers can get this kind of development to try it. To avoid such a trap, makes a beeline for use SSL-or TLS-encoded correspondence stages[17]. Rather than misusing support surge and expanding complete access to a database in the essential stage, cybercriminals routinely play a round of Hopscotch: finding an inadequacy inside the establishment that can be used as impact for more honest to goodness strikes until they accomplish the back-end database system. Case in point, a software engineer may worm their way through your records division before hitting the Mastercard taking care of open air theater. Unless every division has the same standard of control, making separate chairman accounts and isolating frameworks can alleviate the danger[6].

Presently what we do was we take the following most regular method of B2B e-trade as an illustration. As in the Fig 1 the stream is as B2B e-business framework. In this we can see that the procedure client submit to the database server might be protected.[1] There may be plausibility that the outsider can take the secret word with the assistance of insight question and gets the clients data subtle element.

The watchword gets effortlessly be grabbed by the programmers so the security on secret key has not been finished. We can likewise have stream diagram of recuperation secret key.

The hint password that we are using is not encrypted which will lead to insecurity of database system. So we uses a hybrid encryption technology which uses symmetric and asymmetric encryption technology.

Aditi Gupta,AIIT, Amity University Uttar Pradesh, Noida

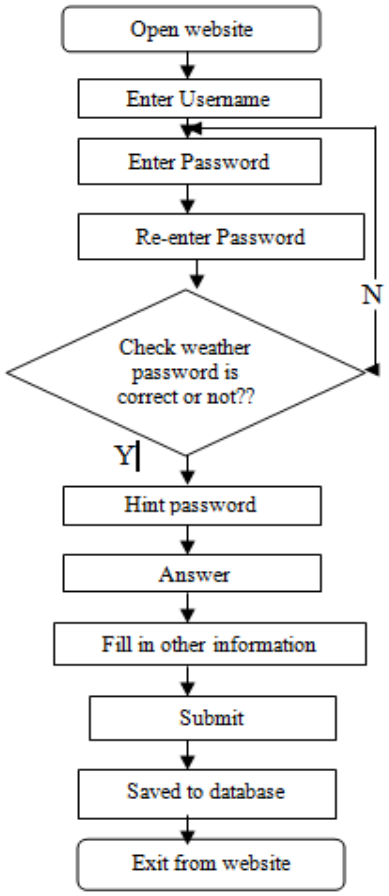

Fig 1: User Registration Flow Chart

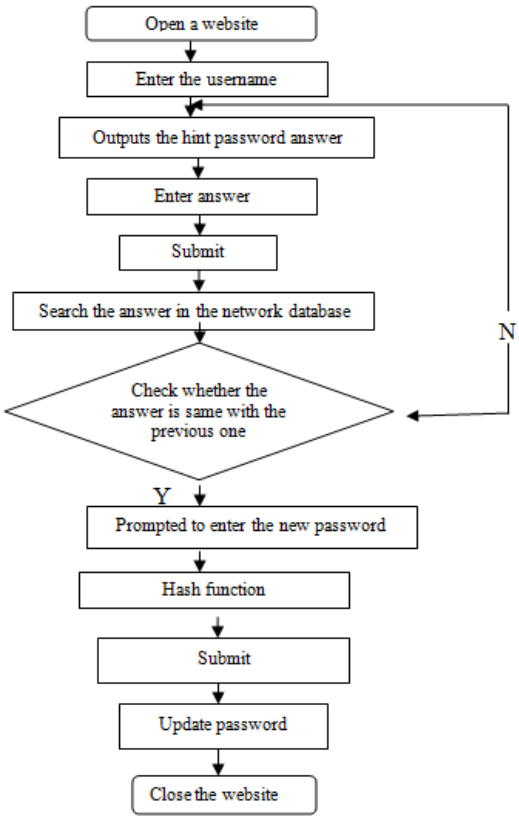

Fig 2: User Recover Password Flow Chart

III. HYBRID ENCRYPTION TECHNOLOGY

In this technology we have discussed about the symmetric encryption and asymmetric encryption and lastly the hybrid technology.

A. Symmetric Encryption Technology

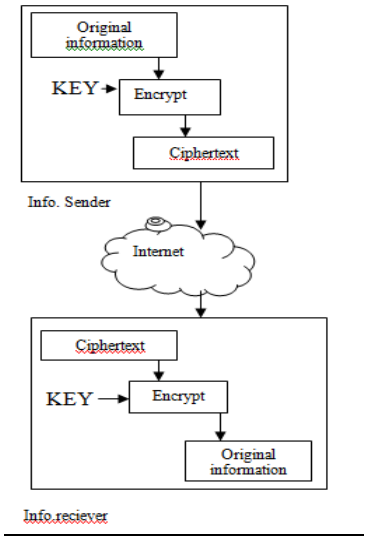

Fig 3: Symmetric Encryption

The above depicts the schematic when sender sends the data in a scrambled structure utilizing a few calculations and key as a part of which the first data gets changed over into Fig content.

Presently at the season of recipient the unscrambling utilizing the same calculation and key and change over the Fig content into unique data. The most well-known calculation which is most broadly utilized is DES which is known as information encryption standard. This calculation is proposed by IBM company.[3,4] The fundamental procedure as it first supplant the area of ciphertext64 bits and gets unequivocal gathering of 64 bits and partitioned into 32 bits each L0 and R0. After that the execution happens of L0 and R0 after that two sections yield will come at sixteenth position and get the outcome. The essential procedure is as per the following.

Having a symmetric encryption prompts favorable position as having a rapid and high effectiveness. It is utilized when there is extensive measure of information and it additionally conation a detriment that the keys are effectively gets deciphered over the system. When we are utilizing a symmetric encryption keys thought about.

1) Initial permutation: Replace the location of cip hertext of 64 bits and get an out-of-order explicit group of 64 bits. It is divided into two paragraphs of 32 bits. L0 and R0 are respectively used to express.

2) Execute the following iterative transformation to L0 and R0: Li = Ri-1 Ri.= Li-1⊕f (Ri-1,Ki) i=1,2,…,16

3) Two parts output after the 16th transform exchange

order, do inverse initial permutation and then cipher text will result.

B. Asymmetric Encryption Technology

In this a sender is sends the first data encodes it utilizing an open or private key and give yield as a Fig message and do likewise utilizing Fig content as information and gives yield as unique data with the assistance of keys and decode ion.[1] The most broadly utilized calculation is RSA calculation which is proposed by R.Rivest, A. Shamir and L. Adleman. In this the calculation is expand on hypotheses of decay of vast numbers and discovery of prime numbers in this firstly we have to choose numbers, for example, p and q then we have to compute the mathematical statement and in conclusion we have to choose a whole number and illuminate the comparison.

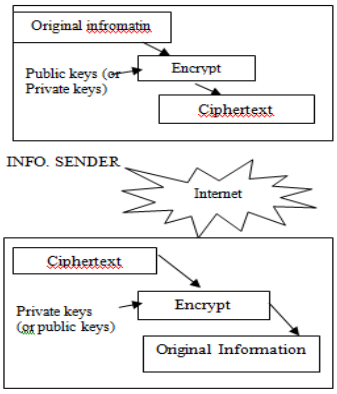

Fig 4. Asymmetric Encryption

An asymmetric contain one advantage that the keys it is using s easy to manage and one disadvantage as the complexity increases and speed gets slower down.

C. Hybrid Encryption Technology

As we had learned about the symmetric and deviated encryption innovation and thinking about their quality and shortcomings so what we have done was we joined them two and made a half breed encryption innovation as appearing in Fig[5].

In this what we are seeing was the utilization of symmetric calculation which utilizes an encode content to ensure transmission security of open key of B as a specific key is scrambling so no other key will decrypt.[5] In the second Fig we can see the utilization of private keys to unscramble the Fig message and gets the symmetric key to encode the documents.[7] With the assistance of this we can see that cross breed innovation conquers the inconveniences and both are completely incorporated.

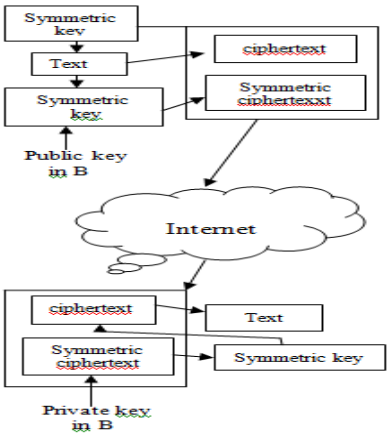

Fig 5. Hybrid Encryption

In view of the above steps, get open key {e,n} and private key {d,n}. Thereinto e is encryption record and d is unscrambling file. Bunch each content, quality is m. Require m not as much as n. Encryption and decoding operations are as per the following.[6] Encryption: c = me mod n Decryption: m = cd mod n The benefit of topsy-turvy encryption innovation is simplicity of key administration. Drawbacks are the intricacy of encryption calculation and moderate encryption. The alogirthm describes.

- Select confidential large numbers p and q.
- Calculate n = p * q,φ (n) = (p-1) * (q-1). There into φ (n) is Euler function value of n.
- Select an integer e, satisfy 1 < e < φ (n) and e and φ (n) are co prime.
- Solve equation d * e = 1 mod φ (n) and calculated

A deviated hold numerous particular case advantage that the keys it will be utilizing encountered with urban decay because of deindustrialization, engineering imagined, government login not difficult should oversee What's more one disservice Similarly as those intricacy increments and velocity gets slower down.

IV. HYBRID TECNOLOGY IN E-COMMERCE DATABASE

The issues that were taking before as in Fig [1] and Fig[2] it gets enhance by utilizing the mixture innovation . so we have considered that the enhanced client enrollment contains an insight question and an answer which will now not to be filled but rather it straightforwardly submits by the key K1 to the server and it then beneficiary to K2 open key.[3,4,5] Along these lines the key can't get stole .the security of information will be there[15].

As indicated by the client enlistment the stride process as takes after:

- User will enter the site enter the username and secret key as utilizing symmetric key K1
- Encrypt the secret word
- Submit the secret word to the k1 to the server
- According to username inquiries the secret word encode by K1
- Check for delegacy Exit

As per the recuperate watchword key K2 will be put together by the customer and secret word will be same in the database in the event that they are same they will sent back and decode it gets the intial watchword.

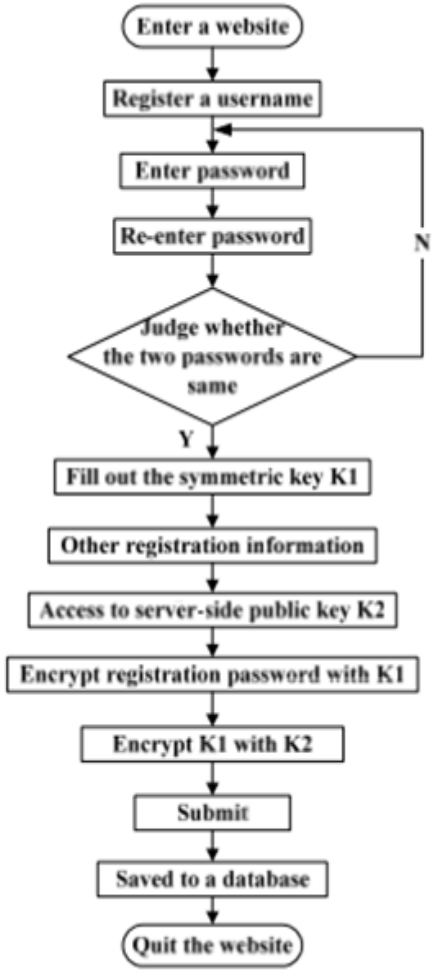

Fig 6: The Improved User Registration Flow Chart

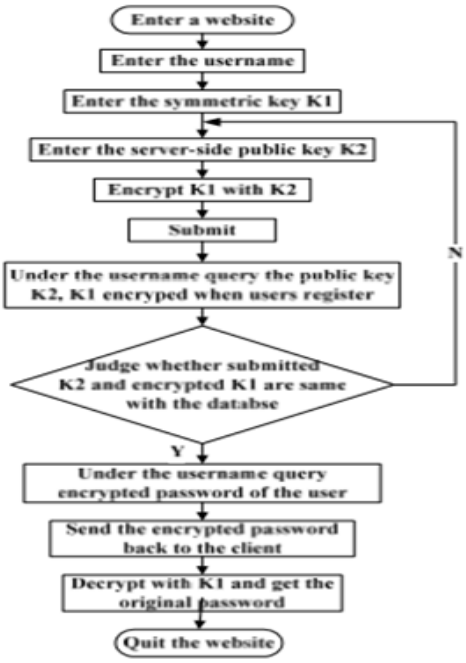

Fig 6: The Improved Flow Chart of User to Recover a Password

V. CONCLUSION

Using hybrid encryption advancement can give full play to the specific focal points of two sorts of encryption count and gives more trustworthy and powerful security for e-exchange structures. The mutt encryption development used as a part of the paper can in like manner be used to overhaul the security of other framework.

ACKNOWLEDGEMENT

Writers express their profound feeling about gratitude of the author President for chloride University, Dr. Ashok k. Chauhan for as much sharp enthusiasm toward pro-moting research Also have constantly been a impulse for accomplishing incredible statures.

REFERENCES

[1] Niranjanamurthy M "E-commerce Security Issues" Advanced Research in computer and communication engineering vol.2 issue 7 july.
[2] Ziff Davis."E-commerce" software world vol. 30 2003.
[3] Y.P.Hu Symmetric cryptography machinery press, 2002.
[4] Abdeldime M.S. Abdelgader, Lenan Wu, Mohamed Y. E. Simik and Asia Abdelmutalab" Design of a Secure File transfer System Using Hybrid Encryption Techniques"2015.
[5] Abdul Monem S. Rahma, Rabah N. Farhan, Hussam J. Mohammad" HYBRID MODEL FOR SECURING E-COMMERCE TRANSACTION" Nov-2011.
[6] Prakash Kuppuswamy, Saeed Q. Y. Al-Khalidi" Securing E-Commerce Business Using Hybrid Combination Based on New Symmetric Key and RSA Algorithm" Vol.20 2011.
[7] Arnon Sturm, Jenny Abramov, Peretz Shoval" Validating and Implementing Security Patterns for Database Applications"
[8] Shelly Rohilla, Pradeep Kumar Mittal" Database Security: Threats and Challenges"vol.3 may2013
[9] Vahid Khodabakhshi Hadi Halvachi"Outsourcing" Dec,2012.
[10] Dr. Laxmi Ahuja, "Inclusion of Information Technology in Supply Chain Management" Biannual journal called 'Journal of Management & IT', ISSN: 0974- 2093, published by MERI, 2009, pp 122-123.
[11] Dr Laxmi Ahuja, "Ontologies-Cum-Computing in Business Application Domains" Annual Journal of Management and IT, 2009, Vol. 3, No. 1, pp 89-92.
[12] S. Kumari and J. Chawla, "Comparative Analysis on Different Parameters of Encryption Algorithms for Information Security," 2015
[13] S. Challenge, J. Zhang, D. Zhang, and A. Drew, "Number Theory Applied to RSA Encryption," 2015.
[14] T. Okagawa et al., "Ip packet routing mechanism based on mobility management in a ipbasednetwork," 14th International Conference on IntelligenceinNGN, 2009.
[15] Chung C Y,Gertz M, Levitt K. DEMIDS: A Misuse Detection System for Database Systems. In:The Third Annual IFIP 11.5 Working Conf. on Integrity and Internal Control in Information Systems, 2009
[16] Rung Ching Chen, Cheng Chia Hsieh. An anomaly intrusion detection on database operation by fuzzy ART neural network. Proceedings of ICS 2003. 839-844
[17] P. Jokela, R. Moskowitz, et al. "Using ESP transport format with HIP", (draft-04), 2007.10