International Journal of Pure and Applied Mathematics
Volume 117 No. 22 2017, 161-165
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Protect The Web Database From Web Instructions and Query Attacks

K.Priya[1] A.Sivasangari [2] Karunya Rathan[3]

[1,2,3] Department of IT, Sathyabama University, Chennai 600119
priyakrishnaskp@gmail.com, sivasangarikavya@gmail.com and n.karunya@gmail.com

Abstract

Nowadays, business applications and information systems are mostly build over web as frontend to be available and accessible to the customers, organizations and business partners located in all over the globe. Also, this is coming under a digital economy, which is growing rapidly in the global economy. End users can access this web application anywhere in the world easily and along with vulnerabilities also a major thread on customer and end users side. There is an outsourced database prototype called TrustedDB which allows clients can execute SQL queries and there will be under agreed and accepted compliance without trusting the service providers. TrustedDB accomplishes this by utilizing server-facilitated sealed trusted equipment in basic inquiry preparing stages. SQL Queries allow attackers to access unofficial data (read, insert, change or delete), gain access to privileged database accounts. In this paper, we thus propose to make trusted hardware a first-class citizen in the secure data management area.

Keywords—; Data Privacy, Data Confidentiality, security vulnerabilit,; query processing**.** .

1.INTRODUCTION

Numerous Scenarios of data leaks in the recent years have made the Clients to place their valuable data's in a third party provider without the assurance of providing the privacy and data confidentiality. Data privacy means the data owned by an individual will never be disclosed to anyone else. Whereas, the data confidentiality refers to the ability to share the sensitive data among a community of users. This provides the safety of the database from the hackers (intruders, insiders and administrators). Privacy is always a bit easier to implement rather than implementing the data confidentiality. It is a tough task to implement both the security attributes to the database. There occur several problems with the modern day database that the hackers can hack a database by Bypass login i.e. they hack the user login details by cracking the username or password and entering into the user database. Also, the administrator can also view the database which can be of a danger to the client data. There is a possibility of data leaks. This can only be controlled by providing the data confidentiality and the privacy at the same rate. We have introduced the concept of placing the SCPU (secure co-processor) outside the main database thus it doesn't have any limitation to the memory space of the database along with which the Concept of paging module is implemented for the ease of the database query parsing. The main objective is to keep database in a well secured manner under serious SQL injection attacks and to analyze the principle of SQL attacks. It gives more secure and safety modes to users and administrators. The contributions of this paper are 1.) Provide privacy and data confidentiality to the Clients 2.) Reducing the process of hacking by the hackers to a certain extent. 3.) Providing the Transfer Secure Schema to the data.

The problem of the hacking can be controlled by converting the username and password into the 16bit digit by using the MD-5 algorithm whose output is converted into raw data and this raw data stored into the database so that the chance of bypassing the user account can be nullified. Hackers mainly target the code of the database where the username or the password of an user can be easily hacked this can degrade the database security and it can be rectified by saving the username and password not as such instead they are stored in the converted manner. At the position of providing the information to a database there is a possibility of modifying the database or deleting its data's by code injection. This Possibility of modifying the database by SQL code injection can also be avoided by using the Bind variable method. Whereas, by the usage of dbms-assert each query is processed word by word which avoids running various function. Recent problems with the administrator viewing the data and compressing the privacy can be rectified by using the concept of wrapping to provide the secure transfer of data and also to secure the data storage.

2. RELATED WORK

B. Bhattacharjee,et al[1] have described a solution for sharing and mining of data with privacy using coprocessors which are secured through cryptography but are resource limited. E. Mykletun,et al[2] have suggested a method for encryption of aggregation queries other than the homomorphic encryption technique which is vulnerable to the cipher-text attacks. R.A. Popa, et al[3]have introduced CryptDB which is a framework that gives reasonable and provable classifiedness even with the assaults for applications upheld by SQL

databases. It meets expectations by executing SQL questions over scrambled information utilizing a gathering of productive SQL-mindful encryption plans. CryptDB can likewise anchor encryption keys to client passwords, so that an information thing can be decoded just by utilizing the secret key of one of the clients with access to that information. Subsequently, a database manager never gets access to unscrambled information, and regardless of the possibility that all servers are traded off, an enemy can't unscramble the information of any client who is not logged in.

K.Priya et al [4] have described the context term frequency where collected the user related information to produce the multimedia proposal system for video redundancy avoidance. S. Bajaj ,et al [5] have presented TrustedDB, an outsourced database model that permits customers to execute SQL questions with protection and under administrative agreeability requirements by utilizing server-facilitated, sealed trusted equipment in basic question handling stages, subsequently uprooting any limits on the sort of bolstered inquiries. G. Aggarwal, et al [6] have proposed a dispersed building design that permits an association to outsource its information administration to two untrusted servers while safeguarding information security. We indicate how the vicinity of two servers empowers effective apportioning of information so that the substance at any one server is ensured not to break information security. K. Priya [7] Different video frames are analyzed over Ontology, also provides the topological, spatial and temporal on videos. Overall semantic content on the videos has been achieved by performing this action. V. Ganapathy, et al [8] have presented TrustedDB, an outsourced database model that permits customers to execute SQL questions with security and under administrative consistence imperatives by utilizing server-facilitated, carefully designed trusted. Equipment in discriminating inquiry handling stages, in this manner evacuating any restrictions on the sort of upheld inquiries.

3.PROBLEM DESCRIPTION

In this section, we have formally defined the security primitives used in this paper to provide the ease of architecture a thereby enabling to provide the privacy and data confidentiality to the database..

3.1 Message Digest Algorithm (MD5)

MD5 is a hash function which was developed by Rivest. It generates a 128 bit long message and followed by a hash value. It is based on the principle of Merkle-Damgard construction. This MD5 is not, like the MD-4 which is the forerunner of MD5, which is an iterating three-round hash function, but this has been expanded by a round among all other things. Thereby it said that the MD5 function has slightly decelerated in contrast to the MD4 function.

In summary, we may say that the essential differences between the two versions are, on the one hand, where the expansion of the compression function from 3 to 4 passageways and, on the other hand, where the addition of an additive constant per step and not hitherto 2 additive constants. Of course, still there are much more differences which, however, need a lot of understanding about the matter and they are not reasonable to be mentioned here. we have implemented this concept of MD5 in our paper for providing the 16bit digit output of numerical values.

3.1.1 Functionality of the MD5

Initially, the message is raised to the multiple of 512 through the concept of padding. Where the message should be congruent with 448, and modulo 512. Hence, this can be emanated from this that the message has always exactly 64 bit and is also a bit smaller than a multiple of 512 of exactly these 64 bit. Firstly, 64 bit coded numbers will be affixed once 1-bit and 0-bit sequence is appended. Then, a cache consisting of the 4 registers A, B, C and D, where each of them having 32 bit, is initialized and setup. Now the first 512-bit block runs through the following four rounds consisting of 16 operations:

f (X,Y,Z) = X and Y or not (X) and Z
g (X,Y,Z) = X and Y or X and Z or Y and Z
h (X,Y,Z) = X or Y or Z
i (X,Y,Z) = Y or (X not (Z))

The MD5 hashing algorithm is used to check the data integrity over 128-bit message which created from input data. The data given as input is fingerprint of a specific person and unique. Bind variables are key for the application performance and those are the Oracle concepts.MD5, which was initially developed by Professor Ronald L. Rivest from MIT, which is intended for use along with digital signature applications, it requires that a large amount of files must be compressed by a secure method before that is being encrypted along with a code of secret key, under the public key cryptosystem. MD5 is currently a standard for conversion, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321.

Step1: Appending Padding Bits:

At this phase the original message is padded so that the length is congruent to 448 of modulo512.Following are the Rules:

1. Original message is always padded with one bit “1” first.
2. Zero or more bits ”0” are padded to bring the length of the message up to 64 bits fewer than multiple of 512.

Step 2: Append length

Here initially, 64 bits is appended along end of the padded message to indicate the length of the original messages in bytes. Following are the rules.

1. Length of original message is converted to its binary format of 64 bits.
2. Break it into 2 words (32 bits each)
3. Lower order is appended first followed by second

Step 3: Initializing MD5 Buffer

It requires 128 bit buffer with a specific initial value.

Buffer divided into 4words
A->0*67452301

B->0*EFCDAB89
C->0*98BADCFE
D->0*10325476

Step 4: Processing Message in 16 word blocks

For each input block 4 rounds of operations with 16 rounds in each round are performed.

F(X, Y, Z) = (X AND X) OR (NOT XAND Z)
G(X, Y, Z) = (X AND Z) OR (Y AND NOT Z)
H(X,Y, Z) = X XOR Y XOR Z
I(X,Y,Z) = Y XOR (X OR NOT Z)

Algorithm: for K=1 to N

T[1,2,…….64] Array of special constants
T[i] = int(abs(sin())*2*32)
M[1,2,……N], Block of padded & Appended message
R1 (a, b, c, d, x, s, i)
Round 1: a = b+((a +f(b ,c, d)+X+T[i])<<S)
R2 (a,b,c,d,x,s,i)
Round 1: a =b+((a+G(b,c,d)+X+T[i])<<S)
R3(a,b,c,d,x,s,i)
Round 1: a = b+((a+H(b,c,d)+X+T[i])<<S)
R4(a,b,c,d,x,s,i)
Round 1: a=b+((a+I(b,c,d)+X+T[i])<<S)

Step 5: Content in Buffer words

A, B, C, D are returned in sequence with lower order byte first. MD5 comprises of a number 64 of these operations, which are assembled in four rounds of 16 operations. Where F is a nonlinear capacity; Mi means a square of 32-bit message data, and Ki indicates a consistent of 32-bit, where diverse for every operation.<<s means the pivot of left bit by s places; s fluctuates with every operation 232.

3.2 Raw Data

Raw data (also known as primary data) is a term which is used for data collected from a source. These raw data has not been subjected to processing or any other manipulation, and are they also referred to as the primary data. This raw data can be input to a computer program and also used in manual procedures such as analyzing the statistics from a survey. This term can also refer to the binary data which are present on the electronic storage devices such as hard disk drives (also referred to as low-level data).

In computing, raw data may have the following attributes: They might possibly contain errors, which are not validated in different (colloquial) formats; they might not be coded or unformatted; and also suspect, requiring the confirmation or citation. For example, the data input sheet may contain dates as raw data in many forms: "29th January 1994", "29/01/1994", "29/1/94", "29 Jan", or "today". Once when captured, these raw data could be processed and stored in a normalized format, perhaps the Julian date, so as to be easier for computers and humans to interpret them during later processing. Raw data (also called "sourcey" data or "eggy" data) are the data input to processing. Where a distinction is made at sometimes in between data and information to the effect. That this information is the end product of data processing. Raw data which has undergone processing are referred to as "cooked" data. Although these raw data has the potential to become "information,". The extraction, organization, and sometimes analysis and also the formatting for presentation are required for this to occur.

3.3 DBMS Assert

SQL injection is a code injection technique that takes advantage of loose coding of database applications.

- First Order Attack: Here the User enters injection code and gets a different result .
- Second Order Attack: The User injects code into the database, when it is run for the next time someone else will display that data.
- Blind or Inference: Here no information's are presented directly, although it is possible to infer the information based on the repeated results and also based on loose error trapping. These Repeated tests also allow information to be gathered whether it is the first number of the credit card.
- Compounded: Here the process of SQL Injection is used in conjunction with other techniques in order achieve a specific goal. For example, The

goal may be to create a Denial Of Service (DOS) attack.

3.4 Wrapping

The PL/SQL Wrapper process converts n PL/SQL source code into an intermediate form of the object code. Thus by hiding the application internals, this Wrapper prevents the Misuse of the application by other developers. Exposures of the algorithms to business competitors are also avoided. Wrapped code is as portable as source code. The PL/SQL compiler recognizes it and loads the wrapped compilation units automatically without any prior information. Other advantages include Platform independence, Dynamic loading, Dynamic binding, strict dependency checking, Normal importing and exporting.

3.5 Bind Variable

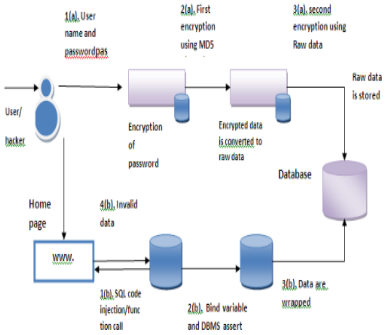

Fig. 1. System Architecture Model of the Trusted DB

Bind variables are key for the application performance and those are the Oracle concepts. Once a query is submitted the Oracle first checks in the shared pool to see whether the statement has been submitted before. If already executed the execution plan is retrieved and the SQL is executed.

4.CONCLUSION

We have provided Architecture for Trusted DB where both privacy and data confidentiality are involved at the same ratio and this architecture provide the advantage of avoiding the unauthorized access to any application and also addition of the SQL statements and the calling of an oracle function are also avoided by implementing this architecture. Thus they also provide the security to the database from both the hackers and also from the administrator of the database. Thus involving this concept of using the SCPU as a master and not as an slave and also placing this SCPU out of the database provides comfort as there are no restrictions of memory usage.

5. FUTURE ENHANCEMENT

As this concept of Trusted DB is now implemented in oracle 10g. In the near future this concept of Trusted DB can also be implemented in the cloud. It might provide better results for enabling privacy and data confidentiality to the database at low cost in the upcoming years. This might come in handy for the organizations who are building up their databases in cloud at that time. Though the protection of database in a small area of network has been achieved using these concepts, it should be achieved in a wide area of network. The SQL protection as well as recovery of the information should be achieved in an easier manner. The disk space required for storing the data should be partly reduced. The information storage capacity of a database system should be enhanced without leaking out necessary information of a user. The information should be wrapped in a secured manner so that no one can access it. Likewise this database protection system must be enhanced in the nearly future.

References

[1] B. Bhattacharjee, N. Abe, K. Goldman, B. Zadrozny, C. Apte, V.R. Chillakuru, and M. del Carpio, "Using Secure Coprocessors for Privacy Preserving Collaborative Data Mining and Analysis," Proc. Second Int'l Workshop Data Management on New Hardware (DaMoN '06), 2006.

[2] E. Mykletun and G. Tsudik, "Aggregation Queries in the Database-as-a-Service Model," Proc. 20th IFIP WG 11.3 Working Conf. Data and Applications Security, pp. 89-103, 2006.

[3] R.A. Popa, C. Redfield, and N. Zeldovich, "Cryptdb: Protecting Confidentiality with Encrypted Query Processing," Proc. 23rd ACM Symp. Operating Systems Principles (SOSP '11), 2011.

[4] K.Priya,Subitha.N, "Online Video Recommendation With User Behavior and Spammer Detection" in IEEE International Conference on Communication and Signal Processing(ICCSP'15) held during 2nd to 4th ,Apr 2015

[5] S. Bajaj and R. Sion, "TrustedDB: A Trusted Hardware Based Outsourced Database Engine," Proc. Int'l Conf. Very Large Data Bases (VLDB), 2011.

[6] G. Aggarwal, M. Bawa, P. Ganesan, H. Garcia-Molina, K. Kenthapadi, R. Motwani, U. Srivastava, D. Thomas, and Y. Xu, "Two Can Keep a Secret: A Distributed Architecture for Secure Database Services," Proc. Conf. Innovative Data Systems Research (CIDR), pp. 186-199, 2005.

[7] K. Priya, "Effective Extraction of Semantic Content in Videos Using Meta-Ontology" in Journal of Theoretical and Applied Information Technology in vol73(2) Mar 2015 ,pp:296-300.

[8] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R. Motwani, "Distributing Data for Secure Database Services," Proc. Fourth Int'l Workshop Privacy and Anonymity in the Information Soc. (PAIS '11), pp. 8:1-8:10, 2011.