Asian Journal of Information Technology 16 (6): 544-551, 2017
ISSN: 1682-3915

Coalition Technique Protecting Cloud Storage by Shielding it Against Intrusion

[1]D. Seethalakshmi and [2]G.M. Nasira
[1]Research and Development Centre, Bharathiar University, Coimbatore, Tamil Nadu, India
[2]Department of Computer Applications, Chikkanna Government Arts College,
Tirupur, Tamil Nadu, India

Abstract: Protection of cloud stored data from the intruders by providing shield for the cloud data before any attackers intended for attack. We here present access to data in cloud with legitimate cloud control for clients by increasing its reasonable security concerns. Security focusing on access control strategy conveys data identity established techniques for encryption. Thus, in our approach we propose coalition technique for securing data in dual way mode. It involves the procedure of encrypting the entire data of an individual in an intermediary system and then storing them in cloud database by assimilating any two individual data together. It thus, provides dual methodology for assuring security over cloud database and provide armored database. Coalition technique is the combination of dual methods that primarily encrypts the data strongly with any imposed algorithm arbitrarily chosen by the intermediary system and then that data will be merged with another encrypted data of any other individual storage in cloud and will be set flag that can only be known to the intermediary system. Coalition technique is the influential approach for securing cloud from unexpected attacks before it could happen. Our proposed approach armors the chaos of conquering security after the attack happens. Rather than securing after malfunctioning we could create an unbreakable security wall before the intrusion occurs. So, even if the attacker intrudes and extracts data they could have no beneficial data.

Key words: Coalition technique, intermediary system encryption, data assimilation method, armored database, dual mode approach, malfunctioning

INTRODUCTION

In the popular and complex cloud data storage securing the confidential data makes important mission. Even though it is managed in accordance with the services provided, levels of confidentiality, legitimacy and potential of data stored total security for cloud storage will be the intricate task to accomplish. Recently, much trouble arises due to lack in privacy and internet security. In internet the storage or application can be used online and data will be shared with widespread people using cloud space. Cloud is the extensive space for contributing individuals World Wide Web utilization in various fields like banking, cash transactions, social web media communications, travelling guide and for learning purposes (Frohlich and Plate, 2000). The privacy in all these sectors is the big point of issue in the interconnected network system. To accustom this applications and data crisis over wide web services becoming the multi-tier approach for executing the methods. Cloud data is outsourced to the external units in the multilevel design of networking system (Bai *et al*., 2005). The data outsourced have no surety for data protection measures in the outsourced system for various processing purposes. There exist many intrusion detection systems in multilevel web services for detecting attacks if occur by traffic patterns (Debar *et al*., 1999). Various detection systems in web server along with the database server require different techniques for securing database in cloud. Some of the prevention techniques used as security system protecting from occurrence of attacks in the web server.

When any attack happens in the web based database server it creates some other intrusion detection system for deter the database server. It creates motivation for associated web server attacks that has reason for creating some other intrusion detection system to conquer forthcoming attacks. Refrain from devising multiple attack prevention or detection system we can invent web database server attack armoring system that can shield the database before any attack or intrusion emerges (Bates *et al*., 2010; Yu and Lau, 2006).

Most of the prevailing attack detection system individually attacks the web or database server to protect

Corresponding Author: D. Seethalakshmi, Research and Development Centre, Bharathiar University, Coimbatore, Tamil Nadu, India

multilevel web oriented services with efficient intrusion detection system (NVD., 2017). Many web oriented services increases their tasks by providing its applications extensively for personal uses, corporate web oriented applications targeting the attacks. More than attacking the front end application exploitation will be done majorly in backend database without the knowledge of the legitimate user itself. Detection of the intrusion against any database system in the network and extract confidential information will be more common and very difficult to provide data security.

In a multilevel anomaly detection system it produces network behavior patterns in database extraction and interaction over the internet. The multilevel database access aids in remote approach of back end database system with database servers. It prevents remote access towards attacks that are affected by the web requests with web oriented attacks with exploitation of back end database. Data traffic materializes the patterns and signature protecting the multilevel web architecture with intrusion detection model by unidentified attacks. Recognizing abnormal situation arises in database or in the backend without the knowledge of frontend system. Abnormal traffic in the data network deviate the attention of intrusion prevention system and alleviates attack.

Inappropriate handling of attacks forces several attention seeking frontend advertisements prone to web services and corrupt backend database. Constant victim database of attacks will be given more consideration and for every type of attack detected an attack defending and fighting mechanism has been evaluated. It becomes inflation in attack defending and this much scrutiny will affect the web server performance and speed of other database tasks. Independent network functions in a multilevel architecture of web oriented database detecting the anomaly from the attack prone web pages, messages or commands is frequently secluded by firewall protection (Stavrou *et al*., 2009; Tupakula and Varadharajan, 2003). Every individual data packets transmitted in the network will be examined by the created intrusion detection and anomaly detection models. Despite of the protection the issue arises will be the chunks of data packets transferred which has no continuity of the database. So, it could not be that much efficient in finding the difference between legitimate and illegitimate commands or data over the system.

Literature review: According to P. Bhujbal and N.S. Jadhav intervention detection system using double guard technique in broadly used web applications in cloud system in which the modern world applications involve complete online transactions. Web oriented server database will be hacked easily and protected using by the double guard protection system (Wagner and Dean, 2001). It prevents and detects multiple types of attacks using double guard protection system that also uses intrusion detection and secure web server and database server presenting the direction and query detection system. Intrusion detection by modeling the performance of network duration rate between front end and backend behavior of database across double guard system solving the problem of isolating the data flow from every time period of server usage. Accuracy detection calibrates the system by exerting the patterns for static and dynamic web application with database query based approach (Christodorescu and Jha, 2006). In this study, they detect and build interrelated models of websites applicable of active requests with retrieval of updates and database of backend and front end web server.

By defending against injection attacks through context sensitive string evaluation by Tadeusz Pietraszek and Chris Vanden Berghe injects susceptible threat for applications intensity of security provided. Several types of frequent attacks like SQL injection and the vulnerable attacks exploiting the outcome of applications in the error susceptible exploitations. The method for disclosing the prevention of injection attacks by consigning the origin of attacks increasing the improvised serialization of user specified inputs. The platform for accomplishing the separate channels uses sequence of metadata accreditation (Sekar, 2009). Preserving the string operations with context of required application develops the interactions with source code modifications. They state the prototype using CSSE method deployment for efficient type of attacks prone to error.

As stated by Debar *et al*. (1999) towards a taxonomy of intrusion detection system its main goal is to detect attacks across the network against data with common trouble providing secure data. It maintains security for complete database maintenance by utilizing it with operational constraints (Nabeel *et al*., 2013). Secured information system with realization of functional and operational intrusion detection system to check and follow systems management detecting the vision of insecure phase. Efforts for detecting dynamic mislead of the legitimate users with external database system to abuse the exploited privileges that has vulnerable security. It also introduces classification of detecting intrusion that features several aspects of attacking system.

Nabeel *et al*. (2013) defines privacy preserving policy of cloud contents as significant problem that selects the data sharing regarding fine grained attribute based access control functions. It encrypts documents meeting the requirement of the entire policy with various keys using public key cryptography also considered to be as attribute based encryption (Dolev and Yao, 1983). It also explains approach regarding proxy key re-encryption manages efficient appending and revoking of user identities and entities in accordance with the changes and updates in the policies. Same document provides high computational cost with symmetry key applications with cryptosystem using group based on satisfying the policies assigning unique group key having identical vulnerability. Dynamic key cryptography allows users idea with new key management process functioning the broadcast group of key management securing the definition of identical symmetric keys updates the control policies based on some public data in cloud file storage (Boneh and Franklin, 2001).

Boneh and Franklin (2001) justify the Weil pairing method by implementing identity based encryption. It provides cipher text security with random variant model considering the computation model based on bilinear maps amidst its groups. The Weil pairing methods involve elliptic curve mapping that depends on identity plans of encryption and its oriented applications. It specifies random algorithms namely: Setup, Extract, Encrypt and Decrypt. It intuitionally secures parameters and describes definite private key generation. Its original motto is to deploy public key infrastructure using identity based encryption standards denoting key expiration of the system. It revokes public keys and its potential strategy encrypts possible incorporation of public key cryptography. The IBE system application delegates the decryption keys and manages user credentials and the acts as a strong security model.

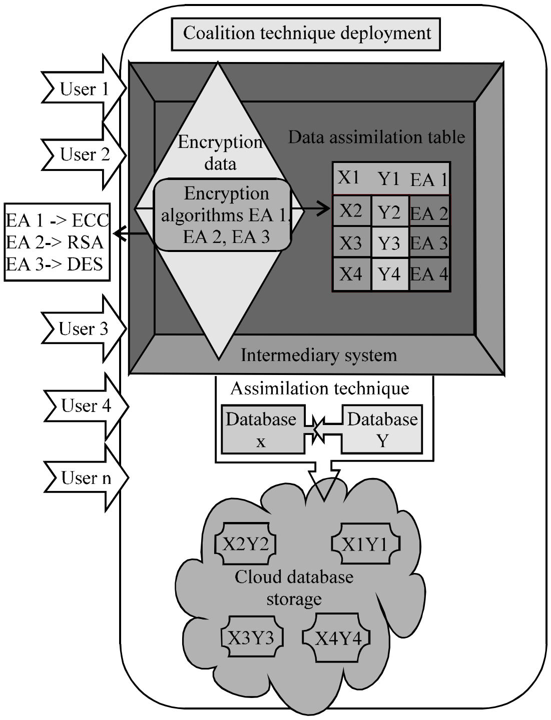
Efficient black-box method used by Sekar (2009) to defeat the web application attacks exploits most of the vulnerabilities caused to the targeted system (Boneh *et al*., 2004). Pragmatic implementation of tracking the defense mechanism helps numerous facts involved in performance overhead issues, instrumentation requests, impact of potential and robust applications and stable specifications for limitation bearing. This study intercepts the requirement of source code protecting this technique attained using the interposition of developing policies used by accurate syntactical injection attacks. It mainly helps detecting wide attacks prepared in other languages.

MATERIALS AND METHODS

Coalition technique deployment: To overcome the security concerns regarding cloud database storage most of the attack detection system have specific check for each type of attacks variedly. Variety of attacks is enduring such as explicit browser attack, attack by Brute force, escalation of privileges, hijack of forthcoming sessions attack, etc. According to the size and effect of attack the detection system will work. Thus, to protect the cloud database in a multilevel web service architecture efficiently we require attack detection and prevention before even the attack proceeds to attack. It should also control dynamic web access towards the database without even linking to the front end web page. As cloud dynamic approach allows the constant modification and extraction of database by using entities and attributes with variables that are satisfied by the user inputs it requires strong prevention mechanism. The mechanism we devise should armor the database from both static and dynamic attack possibilities. Rectifying the problem of creating multiple defense mechanisms for each category of attacks instead we have to integrate and prevails single enclosed protection system.

In the proposed approach we deploy coalition technique imparts shielding over the cloud database storage. It armors the cloud database strongly by the coalition technique using dual methodology focusing on access control approach. Many security concerns regarding storage and retrieval of data from common online storage exist. After the existence of remarkable online transactions the necessity for protection also increases. Coalition technique alleviates and reduces havoc caused by attack or intrusion of external factors. Even though the attacker finds new techniques and attempt the database will not be affected. This technique requires finding accuracy of the legitimate database users and keep away from anomaly of intruders. The performance of coalition technique is immensely competent for determining lively attacks.

Figure 1 we represent how the coalition technique has been implemented in our research. The user data will be encrypted using any of the randomly chosen strong security algorithms and its algorithm code will be noted. Along with that information the two data of distinguished individual users will be renamed as code will also be stored in a table. The intermediary system thus encrypts and maintains table for identification of codes and flags set. It does not have any particular information of any user data. Then according to the two encrypted output selected those cipher text will be assimilated into single database record by denoting its codes accompanied. Merely now the cloud database consist of encrypted coded data that is assimilated with another coded data which does not give any meaningful information and also cannot be distinguished by any means. The encryption standards will also be unpredictable by the user as it has different algorithms used for different data.



X1	Y1	EA 1
X2	Y2	EA 2
X3	Y3	EA 3
X4	Y4	EA 4

Fig. 1: Deployment representation of coalition technique

We implement strong security algorithms such as Elliptic Curve Cryptography (ECC) algorithm, Rivest-Shamir-Adleman (RSA) algorithm and Data Encryption Standard (DES) algorithm. These are public key cryptographic encryption assuring confidentiality of messages use receivers public key to encrypt the message content. The enciphered text will be transferred to the receiving end and there it will compare with its private key and decrypts the message. It thus, maintains high confidentiality where only the receiver with private key can decipher it, the decryption cannot even implemented at the senders end. User data can be communicated only in this stage of coalition technique.

Users can send data to the intermediary system which does not store or retrieve any data from database records. The intermediary system will encrypt the user data and rename it according to its reference and then maintains the reference table which stores the reference name along with which the data is going to be assimilated and the cryptography algorithm used for encrypting that data. Consequently the data will be assimilated together along with bookmarking two data sets by using their reference name and this fully armored data will be sent to the cloud for storage. In the cloud database it is completely shielded and hence of no usage to the intruder. In the further studies the dual methods will be completely analyzed and discussed in detail.

Arbitrary encryption and assimilation at intermediary system: The algorithm specially focuses on the dual shielding method before storing in dynamic database. The entire shielding process will be done in the intermediary system which handles only cryptography and assimilation process and would not store any data in this system instead it only deals with its references. The first and foremost method is to encrypt and convert the data into encipher text which could not be converted to its original form freely. Cryptography is the essential data protection technique in the dynamic network helps data storage and retrieval without any problem. Data will be more protected without any hoax or deceit information moreover it ensures data integrity in most of the online applications. Regardless of increase in the field of securing data and its transmissions facilitating public key cryptography its used in wide spread cloud dynamic database storage securely store data without any invasion or intrusion of interlopers.

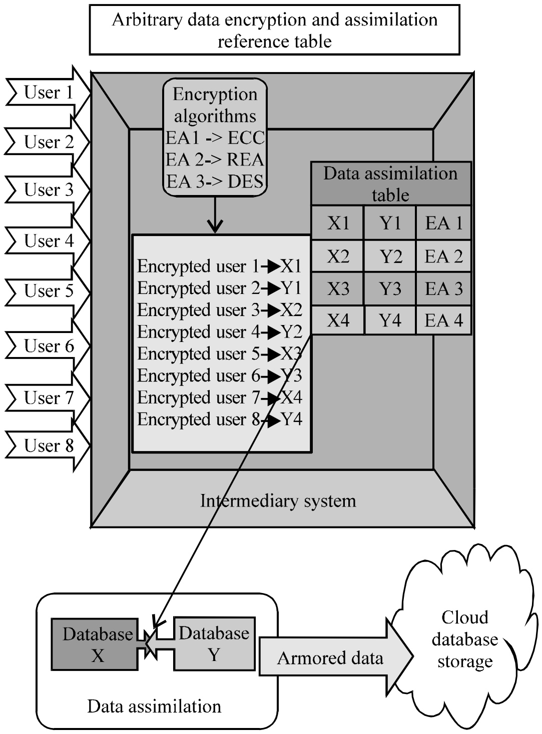
In cryptography public key cryptographic encryption method is one of the hard core encryption and conversion of data into cipher text format which is very hard to interpret. Thus, here we use this kind of cryptographic techniques thus to enable obstruction over illegitimate interlopers accessing the sensitive data. Even if they manage to interlope they will get only trash data which is of no use to them or they could not revert it into its original format without legitimate key. Therefore, we here deploy three different public key cryptography techniques that can be chosen by the intermediary system arbitrarily when the new data entered the system for storage. Here, we simplify the complexity of data security by just giving the processing functions and its reference links to the intermediary system we inculcate for armoring database process. Even if the intermediary system is hacked the eavesdropper could not extract any valid data from it. This system is completely dedicated to convert data text into machine encoded cipher text and then reference table maintenance about the technique of encryption used and the two databases to be merged and assimilated together into a single database. According to its reference link the process will be executed.

The cloud security services concern the data encryption before storing it inside the cloud that destine confidentiality in cloud storage services with generalized data encryption standards beside less usage of size, little CPU time and less usage of memory. Commonly cryptography uses complex algorithms and computational calculations for encryption and decryption so cracking is impossible which needs ample processing power and memory capacity of the hackers system. In our coalition technique we prefer three types of public key cryptography algorithms namely ECC, RSA and DES that are considered as the strong security algorithms.

Elliptic Curve Cryptography (ECC) algorithm is an efficient encryption algorithm that shares public key securing the cloud database with small key size and increases security level. We use 256 bit ECC public key cryptography that gives complete security based on discrete logarithmic calculations difficult for equivalent key lengths. It mainly uses elliptic curves at instances of polynomial time algorithms and exponential time algorithms. Small calculable computations involve polynomial time and complex computations evaluated using exponential time algorithms. The ECC equation depicted as $y^2 = x^3+ax+b$ where generation of public and private key is imposed. Random generation will be used for public key and the range will be selected from 1 to n-1 where the curve point generates both public key and private key. Secured ECC computes elliptic curve point as output and encrypt this output from the previous curve as information to be exchanged with the next point of curve. Likewise, it uses about 32 elliptic curves for encrypting information. It requires less block size, key size and parameters to produce strong security system for database.

RSA algorithm deploys key exchange and digital signature verification procedures with several digits and calculations create public key and private key pair as security solutions. The procedure for RSA key provision involves any two prime numbers x and y that is used for valuing modulus n = xy. The other sparingly prime number denoted to be e which will be the exponent forms (x-1) (y-1). From this notion an integer i is calculated and this i will be a public exponent key. The public key (n, e) is computed and it is impractical to determine i from n and e where x and y are large numbers. The message encryption with public key creates cipher text C along with the receiver that has decryption key for further decoding of cipher text. It mainly uses modulus calculations for implementing encryption and decryption which in turn have no other possible calculations without proper key for deciphering it. Thus, it is considered to be the powerful cryptography algorithms.

The concept of DES that is data encryption standard contributes standard protocols with sensitive data classification of the key used for processing encryption and decryption. DES encryption technique uses 64 bit input integer of original text and 56 bit key parity output integer provided with 64 bit block of data. The original text block will shift each bit of integer around the parity blocks that removes key along with its permutation of original text and its key formation. The DES encryption key will be segregated into 28 halves and each half will be shifted one by one. Then, it reintegrates and compresses modifications to reduce keys from 56-48 bits. This compressed key enciphers the original text block and the shifted halves will be again re-shifted. The original data segregated into 32 bit halves and expands its modification to increase its size as 48 bits integer. Thus, it substitute keys and reduces the original bits and shifts the modified bits. Thus, the output from this half of the data block is swapped and encoded text obtained. This repeated shifting process makes this algorithm a staunch method to decrypt or intrude into (Fig. 2).



X1	Y1	EA 1
X2	Y2	EA 2
X3	Y3	EA 3
X4	Y4	EA 4

Fig. 2: Elaborated illustration of procedures for generating armored data for storage

The arbitrary selection of encryption algorithms will be done by the intermediary system before that it will be flagged and labeled with another name for its own reference. After labeling and new name allocation it will assign the counterpart database to be assimilated with this database. The intermediary system will also maintain table that contains information about encryption algorithms chosen and the two encrypted data assimilated together.

According to the depiction in reference table the process of assimilation will be done. Two encrypted and labeled database will be integrated together into a single database by infusing both data altogether. For example, user 1 and 2 data will be encrypted using EA1 that is ECC algorithm and it will be labeled as X1 and Y1. These two data infused into single database which can be recognized or segregated only by its label flagged. That is the block of enciphered text belongs to user 1 will be flagged as X1 and the block of enciphered text belongs to user 2 will be flagged as Y1 at every place it is infused. This reference identity will be generated erratically by the intermediary system so the interloper could not recognize or categorize the user data from the coded text. In this entire process the actual data will never be stored in the intermediary system for any purpose. It will be directly enciphered and stored by its labeled name only thus to avoid hacking threat to the intermediary system.

After assimilation the resultant data will be absolutely protected and armored robustly. Then that protected, enciphered and assimilated data will be stored in the public cloud database storage. Thus, the exertion of coalition technique generates the strong secured data that have no other way to intrude and it will be absolutely useless even when hacked by any other means. The enciphered text produced can never be deciphered following the armor procedures and revert back to the actual data.

Even the actual user cannot directly extract their cloud stored database they can only extract their actual data from the intermediary system with legitimate login. The process, key used for encryption or decryption, assimilated data everything will be barricaded by the intermediary system to outside users or cloud database access. The intermediary system provides users according to the reference table it will decipher the data and shows only their actual data. Even they don’t know about the coalition process inside the system. Therefore, we achieve accuracy in shielding from data attacks, high performance capability and efficient database protection profitably.

RESULTS AND DISCUSSION

Experimental analysis and performance evaluation: We characterize attack threats and its various types which is also our own assumptions and many prevalent attacks. We intend many experiment set ups to combat against all the possible attacks and it also includes attacks which even cant predicted or blocked by any web server or database servers. Attacks include attack over cloud database, database server, intermediary system attack, injection attack, etc. instead of analyzing the network transmission details between web server and database, we model and devise a prevention plan for defending attacks.

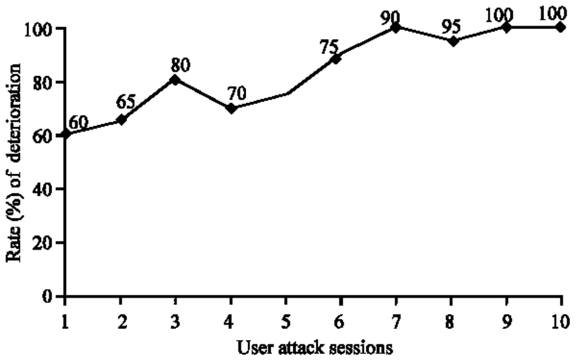


Fig. 3: Rate of deterioration with respect to irrational data contingency according to different user attack sessions

From the storage load tasks in cloud database storage we require internal user attacks to generate new and assumed attacks. It also executes 10 user attacks with different sessions that generate resultant output for armored protection over database. We reach 100% protection of database over shielded protection. According to user attacks their failure in attacking database and their abstraction over irrational data from the secured coalition armored database (Fig. 3).

Rate of deterioration according to different types of user attacks deciding the consistency rate of data contingency and its attack failures. It details the feasibility prototype and cloud services security which cannot be altered or extracted by any other external web applications. The irrationality value depends on how much probabilities the attackers can extract data by breaking cloud storage securities. But, the coalition technique consistency level will be always 100% thus even if the attackers obtain data from cloud storage without authenticated access from the intermediary system they could not have any useful information. The data they gather will be just irrational and of no use. The arbitrary selection of encryption itself makes attackers very difficult to interlope therefore the concept of coalition used in the insulated intermediary system makes it armored. Thus, the deterioration rate will be higher.

Figure 4 shows the performance of deployed coalition technique is analyzed by four factors security, efficiency, consistency and reliability. The security factor in accordance with coalition technique will be very strong due to its dual security method. Efficiency will be much more as the coalition technique implemented is powerful at the same time effective in generating protective data that could not be reverted to its original format. Moreover, it does not occupy more time or space for executing the shielded coalition technique for securing data. When

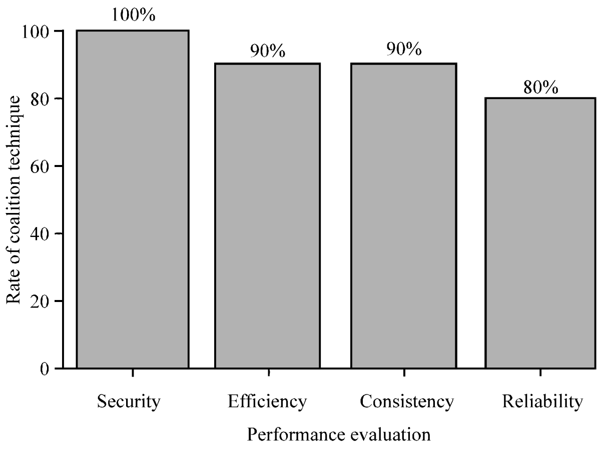


Fig. 4: Performance evaluation of coalition technique

considering consistency coalition assures time consistency, data consistency, security consistency, deployment consistency, etc. As the last matter of fact the reliability over data and the user access is very high. The intermediary system used for deploying coalition technique provides more security and reliability over easy access towards data for the legitimate users. At the same time, it procures hardcore shield over actual data to the external attackers both towards the cloud storage or the intermediary system. Actually, the intermediary system has no data stored in it. Only the link to the data by reference names alone noted thus even the hacking of intermediary system also will not be fruitful for the attacker.

Thus, we provide armored database in cloud storage for which we need not want to worry about any type of attacks, hacks, network congestion, intrusion or any types of interlopers.

CONCLUSION

Along with the accelerated functionalities in network database we face many problems like unauthorized access by illegitimate users. To overcome the problem of security threat against the hackers and attackers from cloud database we propose coalition technique deployment to shield data to be stored in the menace of cloud storage database. In this technique, we use dual shielding methods which are absolutely hack proof which is completely armored. Even if the data is acquired by the attacker it will be completely irrational to them. Thus we provide high security, efficiency, consistency and reliability towards the storage. The deployment of this technique is much more feasible for time, space, smartness or speed than any other security technique. Thus it is the competent and powerful shielding technique for cloud database storage.

REFERENCES

Bai, K., H. Wang and P. Liu, 2005. Towards database firewalls. Proceedings of the 19th Annual Working Conference on Data and Applications Security and Privacy, August 7-10, 2005, Springer, Berlin, Germany, pp: 178-192.

Bates, D., A. Barth and C. Jackson, 2010. Regular expressions considered harmful in client-side XSS filters. Proceedings of the 19th International Conference on World Wide Web, April 26-30, 2010, ACM, Raleigh, North Carolina, ISBN: 978-1-60558-799-8, pp: 91-100.

Boneh, D. and M.K. Franklin, 2001. Identity-based Encryption from the Weil Pairing. In: Advances in Cryptology, Kilian, J. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-42456-7, pp: 213-229.

Boneh, D., X. Boyen and H. Shacham, 2004. Short Group Signatures. In: Advances in Cryptology-CRYPToZ004, Franklin, M.K. (Ed.). LNCS 3152. Springer, Berlin, pp: 41-55.

Christodorescu, M. and S. Jha, 2006. Static analysis of executables to detect malicious patterns. MSc Thesis, Dept of Computer Sciences, University of Wisconsin-Madison, Madison, Wisconsin.

Debar, H., M. Dacier and A. Wespi, 1999. Towards a taxonomy of intrusion-detection systems. Comput. Networks, 31: 805-822.

Dolev, D. and A.C. Yao, 1983. On the security of public key protocols. IEEE Trans. Inform. Theor., 29: 198-208.

Frohlich, B. and J. Plate, 2000. The cubic mouse: A new device for three-dimensional input. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 01-06, 2000, ACM, Hague, Netherlands, ISBN:1-58113-216-6, pp: 526-531.

NVD., 2017. Subscribe to updates from NVD, SCAP, XCCDF and emerging specifications: Announcement and discussion lists. Northern Vision Development, Whitehorse, Canada. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-4333.

Nabeel, M., N. Shang and E. Bertino, 2013. Privacy preserving policy-based content sharing in public clouds. IEEE. Trans. Knowl. Data Eng., 25: 2602-2614.

Sekar, R., 2009. An efficient black-box technique for defeating web application attacks. Master Thesis, Stony Brook University, Stony Brook, New York.

Stavrou, A., C.G.F. Cretu, M.E. Locasto and S.J. Stolfo, 2009. Keep your friends close: The necessity for updating an anomaly sensor with legitimate environment changes. Proceedings of the 2nd ACM Workshop on Security and Artificial Intelligence, November 09-09, 2009, ACM, Chicago, Illinois, USA., ISBN: 978-1-60558-781-3, pp: 39-46.

Tupakula, U.K. and V. Varadharajan, 2003. A practical method to counteract denial of service attacks. Proceedings of the 26th International Conference on Australasian Computer Science Vol. 16, February, 14, 2003, Australian Computer Society, Adelaide, Australia, ISBN:0-909-92594-1, pp: 275-284.

Wagner, D. and D. Dean, 2001. Intrusion detection via static analysis. Proceedings of the IEEE Symposium on Security and Privacy, May 14-16, Oakland, CA., USA., pp: 156-168.

Yu, Y.T. and M.F. Lau, 2006. A comparison of MC-DC, MUMCUT and several other coverage criteria for logical decisions. J. Syst. Software, 79: 577-590.