ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 1 , Issue- 12 , DECEMBER -2015

Research Paper

ENCRYPTED QUERY RESULT THROUGH MAC ADDRESS IN CLOUD

AARTI SHRIVASTAVA[1], SARVESH SINGH RAI[2], NAVDEEP KAUR SALUJA[3]

1. **SCHOLAR, INFINITY MANAGEMENT & ENGINEERING COLLEGE, SAGAR (M.P), INDIA**
2. **ASST. PROF. INFINITY MANAGEMENT & ENGINEERING COLLEGE, SAGAR (M.P), INDIA**
3. **HOD – CSE, INFINITY MANAGEMENT & ENGINEERING COLLEGE, SAGAR (M.P), INDIA**

Abstract-

Now we are living in IT era and now everyone using IT . User host his data in remote, there remain open questions about server. This information is in encrypting form. But user perform search query for retrieve operation, kind of query operations can be performed on the encrypted data. Result appears in client machine. Client machine may be in LAN or in network. So user in same network can access information of computer from same network. In this paper, we focus on how can make safe information of computer from same network computer. When user put query to remote machine it work on IP machine. Most of the user used share IP means one IP have several machine. So in this case we can't analysis unique address of computer, So other computer in same network can access data. Every computer has unique MAC address. With the combination of IP and MAC address we can find unique address of computer. In this paper we will work on MAC address and will encrypt data with the help of MAC address. When data come on correct MAC address then can only readable

KEYWORDS

Cloud Computing, Encryption, Range Query

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 1 , Issue- 12 , DECEMBER -2015

INTRODUCTION

Cloud computing is becoming popular day by day. Its performance is distributed in three main places, one in client's place, one in network and the third is in server's side. As complete data resides outside premises, maintaining confidentiality is becoming an important issue which needs to be addressed. So, security threat is an aspect to think for cloud computing. Data owners now have the opportunity to outsource their data as well as services to the cloud which can provide on-demand access to the data. However, to avoid various privacy concerns or to protect data confidentiality, data owners usually encrypt their data at first place and then outsource them to the cloud. Since the data are encrypted, this places limitations on the range of operations that can be performed in the cloud. The previous paper focuses on the range query. In previous paper result can be used by same network user. Suppose in financial services provide use cloud service. His agent can perform DBMS operation. Because of encryption cloud provider can't see data. But user in same network can view search result in other machine with certain type of attack. Financial data have most secure it can't permit to see by other person. In our paper we focus "DBMS result will be available on same machine which fill request". Data encryption, query security will be according to pervious paper but in our paper new thing only result can view by only machine which fill request. Most of the user and member of organization work on common IP. But every machine has unique ID, which is MAC address. User submit request it will reach to cloud with IP address and MAC address. When result will appear it will check MAC address of viewer machine. If MAC addresses same then he can able to see result. In our paper, prevention of attack is focused. Our system works on client level. No one can access our data through local internet file. In our system data will encrypt by MAC address. Once result will generate it will encrypt with MAC address when it will reach to client machine it will decrypt by machine MAC address

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 1 , Issue- 12 , DECEMBER -2015

CLOUD DBMS

A cloud database management system (CDBMS) is a database management system that is hosted by a third-party service provider on a remote server and accessed over the Internet.

A cloud DBMS can be deployed in three different ways. The first way is as a virtual machine (VM) image. In this deployment model, the cloud provider sells virtual machine instances upon which a database management system can run.

In the second deployment model, the cloud provider is responsible for supplying and maintaining the DBMS.

In the third deployment model, the cloud provider installs, maintains and manages the entire database implementation. When and how to deploy on a cloud DBMS is not a cut and dried proposition. Before deciding whether or not to deploy in the cloud an organization should determine its requirements regarding:

Performance - A cloud DBMS typically will not provide the same level of performance as a locally-implemented DBMS simply because the data must be accessed over the Internet.

Budget - A cloud DBMS eliminates capital expenses for software, hardware and data center costs and translates the required investments into operational costs. For businesses that are launching new database projects or looking to move to a different DBMS, a reduction in upfront costs can be very appealing.

Data governance - If data in a cloud DBMS is distributed across multiple geographical locations, the regulatory compliance burden can become more difficult and impact various aspects of data governance including (but not limited to) privacy rules, disclosure requirements, retention rules and data protection requirements.

Staffing - A cloud DBMS can free database administrators from having to worry about tasks such as configuring and patching an on-premises DBMS and make more effective use of their time. Organizations with small or limited IT teams can benefit from hosting databases in the cloud because installation, management and other administrative issues can be offloaded to the cloud provider.

ISSN: 2395 - 2180 Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 1 , Issue- 12 , DECEMBER -2015

PROPOSED CRYPTOGRAPHY SYSTEM FOR MACHINE -

Whether you work in a wired network office or a wireless one, one thing is common for both environments: It takes both network software and hardware (cables, routers, etc.) to transfer data from your computer to another—or from a computer thousands of miles away to yours. And in the end, to get the data you want right to YOU, it comes down to addresses. So not surprisingly, along with an IP address (which is networks software), there's also a hardware address. Typically it is tied to the network interface card, or NIC. The NIC is essentially a computer circuit card that makes it possible for your computer to connect to a network. Every NIC has a hardware address that's known as a MAC, for Media Access Control. Where IP addresses are associated with TCP/IP (networking software), MAC addresses are linked to the hardware of network adapters. A MAC address is given to a network adapter it is unique.

SESSION OF MAC

A session is a way to store information (in variables) to be used across multiple pages. Unlike a cookie, the information is not stored on the user computer. An established session is the basic requirement to perform a connection-oriented communication. A session also is the basic step to transmit in connectionless communication modes. However any unidirectional transmission does not define a session. Session never save in client side So unauthorized user in same network can't use session of other machine.

MAC address is computer unique ID. We will send MAC address with user request and save it as session in server.

Password Protected Encryption MAC address

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. Without a key, the algorithm would produce no useful result. In encryption, a key specifies the particular transformation of plaintext into cipher text, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes. In our paper we encrypt MAC address at client side.

ISSN: 2395 - 2180

Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 1 , Issue- 12 , DECEMBER -2015

Need for secrecy

In designing security systems, it is wise to assume that the details of the cryptographic algorithm are already available to the attacker. This is known as Kirchhoff's' principle — "only secrecy of the key provides security", or, reformulated as Shannon's maxim, "the enemy knows the system". The history of cryptography provides evidence that it can be difficult to keep the details of a widely used algorithm secret (see security through obscurity). A key is often easier to protect (it's typically a small piece of information) than an encryption algorithm, and easier to change if compromised. Thus, the security of an encryption system in most cases relies on some key being kept secret

Encryption through Keyword

In designing security systems, it is wise to assume that the details of the cryptographic algorithm are already available to the attacker. This is known as Kirchhoff's' principle — "only secrecy of the key provides security", or, reformulated as Shannon's maxim, "the enemy knows the system". The history of cryptography provides evidence that it can be difficult to keep the details of a widely used algorithm secret (see security through obscurity). A key is often easier to protect (it's typically a small piece of information) than an encryption algorithm, and easier to change if compromised. Thus, the security of an encryption system in most cases relies on some key being kept secret.

Client Side Encryption

Client-side encryption is the cryptographic technique of encrypting data before it is transmitted to a server in a computer network. Usually, encryption is performed with a key that is not known to the server. Consequently, the service provider is unable to decrypt the hosted data. In order to access the data, it must always be decrypted by the client. Client-side encryption allows for the creation of zero-knowledge applications whose providers cannot access the data its users have stored, thus offering a high level of privacy.

DBMS Query Result Encrypted Through MAC Address-

User submit input. In which cloud DBMS perform operation. Based on operation result

ISSN: 2395 - 2180 Available online at http:// www.ijemmr.co.in

International Journal of Engineering, Management & Medical Research (IJEMMR)

Vol- 1 , Issue- 12 , DECEMBER -2015

will generate. In our paper we will encrypt query result. This encrypt result will send to client machine. It's mean client side reach only encrypted result. If someone in same network want to access result in unauthorized way can't read data.

Decrypted Query Result in Client Side-

When result come on client machine our application will fetch MAC address of machine. And this address work as a key for decryption. It will try to decrypt query result. If request generate by same machine then this MAC address will work as a key for decryption successfully. If someone in same network try to access result in different machine can't able to read result because other machine have different MAC address. So it can't decrypt result. So our content will be safe from different machine.

EXPERIMENTAL RESULTS

Phase 1 Encryption

Plain text character	Key	Result	Plain text character	Key	Result
b	4	y	o	4	l
a	4	x	e	4	b
n	4	k	f	4	c
k	4	h	r	4	o
i	4	f	m	4	j
g	4	d	h	4	e
d	4	a	u	4	r
t	4	q	w	4	t
s	4	p			

Phase 2 Encryption (with secrect password)

Phase 1 Result as Input	yxkhfkdaxqxfpqlybpbkqcoljyxeoxfkqlhrtxfq
Secret Password	confidential
Result from 2nd Phase Encryption	alxmnnhnqyxqreydjsfxjkowlmkjwajxjthcvlsv

CONCLUSION AND FUTURE WORK

Although encryption is not a new innovation, it is a new IT trend. Cloud already have basic protection in place are considering implementing encryption solutions. Securely encrypted data is completely protecte.

Just as data security is ensured on all devices, encrypting data also provides security benefits during transmission.

Users sending files via email or distributing them via a cloud server can use encryption to ensure that no unauthorized user can view them.

Targeted data theft is one thing, but another way to misuse data is through manipulation. Even though a hacker may have absolutely no interest in the information in question, he or she can manipulate specific data to disrupt corporate communications. If encrypted data is used, the recipient will definitely notice that it has been tampered with.

LIMITATIONS

Disk level encryption is time and space consuming. So disk level limitation is size. Encryption algorithm is fix, so if strength of securities key is not high then hacker can break it.

FUTURE ENHANCEMENT

Now a day's everyone is using web services for all of his need. And user wants to upload his information on online storage because of securities and availability issue. So disk level encryption must be efficient regarding time and space. If user have option to select encryption algorithm then it's not easy to hacker analysis pattern

REFERENCES

R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," in CCSW. ACM, 2009, pp. 85–90.

M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communications of the ACM, vol. 53, pp. 50–58, April 2010.

B. Schoenmakers and P. Tuyls, "Efficient binary conversion for paillier encrypted values," in Proceedings of the 24th annual international con-ference on The Theory and Applications of Cryptographic Techniques, ser. EUROCRYPT'06. Springer-Verlag, 2006, pp. 522–537.

Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," SIAM Journal of Computing, vol. 38, no. 1, pp. 97–139, Mar. 2008.

M. Murugesan, W. Jiang, C. Clifton, L. Si, and J. Vaidya, "Efficient privacy-preserving similar document detection," The VLDB Journal, vol. 19, no. 4, pp. 457–475, Aug. 2010.

W. Jiang and B. K. Samanthula, "N-gram based secure similar document detection," in Proceedings of the 25th annual IFIP WG 11.3 confer-ence on Data and applications security and privacy, ser. DBSec'11. Springer-Verlag, 2011, pp. 239–246.

P. Paillier, "Public key cryptosystems based on composite degree resid-uosity classes," in Eurocrypt. Springer-Verlag, 1999, pp. 223–238.

A. C. Yao, "Protocols for secure computations," in SFCS. IEEE Computer Society, 1982, pp. 160–164.

A. C. Yao, "How to generate and exchange secrets," in SFCS. IEEE Computer Society, 1986, pp. 162–167.

O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in proceedings of the 19th annual ACM symposium on Theory of Computing, 1987, pp. 218–229.

O. Goldreich, The Foundations of Cryptography. Cambridge University Press, 2004, vol. 2, ch. General Cryptographic Protocols.

R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols," in Proceedings of 42nd IEEE Symposium on Foundations of Computer Science (FOCS), oct. 2001, pp. 136 – 145.

D. Bogdanov, R. Jagomagis,¨ and S. Laur, "A universal toolkit for cryptographically secure privacy-preserving data mining," in PAISI '12. Springer-Verlag, 2012, pp. 112–126.

A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, nov 1979.

J. Bar-Ilan and D. Beaver, "Non-cryptographic fault-tolerant computing in constant number of rounds of interaction," in Proceedings of the eighth annual ACM

Symposium on Principles of distributed computing, ser. PODC '89. ACM, 1989, pp. 201–209. [Online]. Available: http://doi.acm.org/10.1145/72981.72995

R. Cramer, I. Damgard,˚ and J. B. Nielsen, "Multiparty computation from threshold homomorphic encryption," in EUROCRYPT. Springer-Verlag, 2001, pp. 280–299.