International Journal of Advances in Computer Networks and Its Security– IJCNS
Volume 5: Issue 1 [ISSN : 2250-3757]
Publication Date : 30 April, 2015

Cryptographic Analysis and Security Issues On Cloud Computing

V Praveen Kumar[1] P Premchand[2] S Raghu[3]

***Abstract*—Cryptography is a process of transforming data to make them secure and difficult to intruders. The past idea of cryptography is only encryption and decryption, this tool is a process to send data for a given request using secret keys(secure routing) but now cryptography involves symmetric key encipherment, asymmetric key encipherment and hashing. Our goal is to implement crypt analysis into cloud computing system, recognize generate in human understandable way. This work shows the risk and problems in cloud computing while implementing the technology (intrusion). Few encryption techniques are importance for this research, experiment design of proposed system and cryptography application. Best effort shows that we can also apply mining techniques on cloud computing to protect from intrusion have not been implemented before. In this paper, a survey while implementing crypt analysis into cloud computing system a challenge of the different security risks an exposed.**

Keywords*— *Cloud Computing Encryption; Cryptography; Homomorphic; Order Preserving; Security;

I. Introduction

Data that can be read without any special measures is called plaintext or clear text hide its substance is known as encryption. Encryption plaintext result in unreadable gibberish called cipher text, the process of reverting cipher text to its original plaintext is called decryption. Cryptography is the science of using mathematics to encrypt and decrypt data and enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient

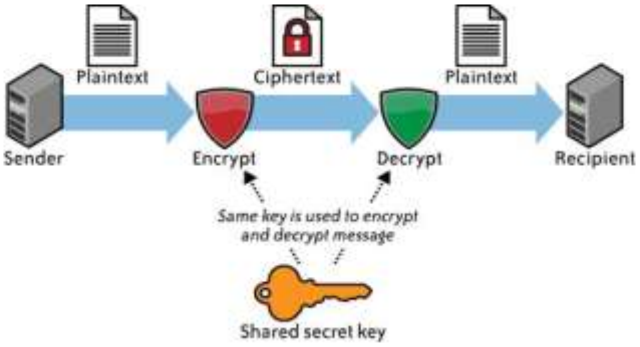


Fig. 1. Symmetric Key encryption

Cryptanalysis is the science of analyzing and breaking secure communication, involves an interesting combination of analytical reasoning application of mathematical tools, pattern finding. A cryptographic algorithm is a mathematical function used in the encryption and decryption process works in combination with a key and converts plaintext to cipher text vice versa. Encrypted data is entirely dependent on two things strength of the cryptographic algorithm and the secrecy of the key. Conventional [2][3] encryption has benefits especially useful for encrypting data that is going somewhere that means for transmitting secure data can be expensive due to the difficulty of secure key distribution. For a sender and recipient to communicate securely using conventional encryption must agree upon a key and keep it secret between them. If they are in different physical locations must trust a secure communication medium to prevent the disclosure of the secret key during transmission. Public key cryptography is an asymmetric scheme that uses a pair of keys for encryption a public key which encrypts data and a corresponding private or secret key for decryption.

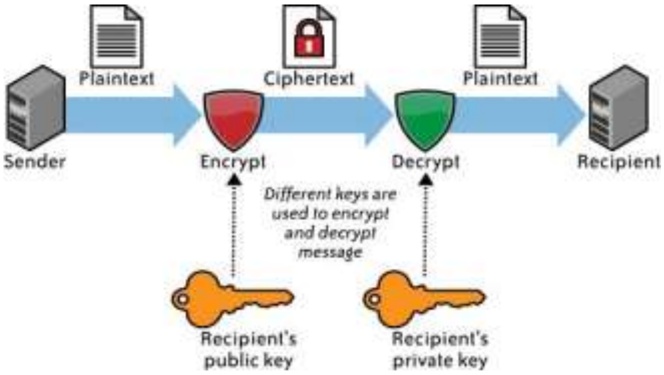


Fig. 2. Asymmetric Key encryption

V Praveen Kumar/ Research Scholar
Department of Computer Science Engineering / Osmania University Inida

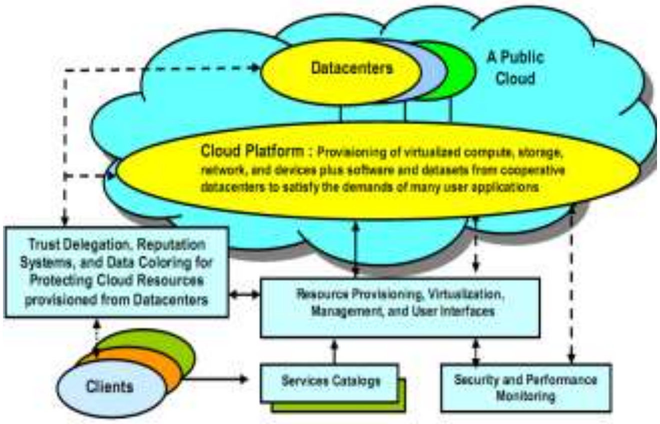
P Premchand/ Professor
Department of Computer Science Engineering / Osmania University Inida

S Raghu/ Research Scholar
Department of Computer Science Engineering / Osmania University Inida

The main benefit of public key encryption is that it allows people which have no preexisting security arrangement to exchange messages securely. Sender and receiver need to share keys via some secure channel is eliminated all communications involve only public keys and no[6] private key is transmitted or shared. PGP combines some best of both conventional and public key cryptography.

Order preserving symmetric encryption is an encryption whose encryption function preserves numerical ordering of the cipher [4] text has single code which lists the corresponding cipher texts in alphabetical or numerical. Order preserving encryption allows data efficient range of indexing and query processing to be exactly as for unencrypted data and locate the desire cipher texts in logarithmic time.

The cloud offers several benefits like pay-for- use, lower costs, fast deployment, scalability, rapid provisioning, , hypervisor protection against network attacks, rapid elasticity, ubiquitous network access, greater resiliency low-cost disaster recovery and data storage solutions, on-demand security controls, real time detection of system tampering and rapid re-constitution of services. While the cloud offers these advantages, until some of the risks are better understood.


Datacenters
A Public Cloud
Cloud Platform : Provisioning of virtualized compute, storage, network, and devices plus software and datasets from cooperative datacenters to satisfy the demands of many user applications
Trust Delegation, Reputation Systems, and Data Coloring for Protecting Cloud Resources provisioned from Datacenters
Resource Provisioning, Virtualization, Management, and User Interfaces
Clients
Services Catalogs
Security and Performance Monitoring

A. *Advantages in Cloud Computing:*

On Demand Infrastructure, Pay as you Use, Reduce cost of Maintenance, Elastic Scaling, Data Centralization, Incident Response, Forensic Image Verification Time,Logging.

B. *Risk in Cloud Computing:*

Data Location, Investigation, Data Segregation, Long term Viability, Compromised Servers, Recovery.

II. CLOUD ENCRYPTION SOLUTIONS

Cloud Encryption Solutions is secure and control access to sensitive data in the cloud while managing encryption keys and access policies. Cloud offers enterprise compelling economic and operational benefits but data security issues need to be addressed to ensure sensitive data is safe.

A. *Cloud Firewall*

Cloud Firewall system prevents unauthorized access to or from a private network either in hardware and software, all messages entering or leaving the intranet pass through the firewall. A firewall is considered a first line of defense in protecting private information for security data can be encrypted.

A cloud based firewall solution can serve the same purpose as traditional firewalls referred as network based firewall. Although there are notable advantages to implementing cloud based firewall solutions moving into the cloud requires careful consideration. It examines the risks threats and level of trust in the service provider. Cloud flare offers three tailored solutions free option a pro and an enterprise option which routed through globally distributed network.

B. *Intrusion in Cloud*

Intrusion detection established themselves as a key component of network security has capability of real time monitoring of network traffic and is intended for identifying anomalies in the network traffic, intrusion system signature database with well-known threats that is used to identify potential suspicious activates. Cloud access provides enterprise class intrusion detection system as well as host intrusion detection is an integral part of the log management components and also integrate with the existing customer.

Misuse detection the intrusion detection system analyzes the information gathers and compares to large databases of attack signatures. Essentially the intrusion looks for a specific attack that has already been documented like virus. Anomaly detection system, administrator defines the baseline or normal state of the network traffic breakdown protocol and typical packet size.

C. *Encryption and Decryption*

Encryption is the conversion of information from cipher text that cannot be understood by unauthorized people and decryption is the process of converting encrypted data into original form, so that authorized users can only understand. Cryptography scheme is assumed to be publically known whereas the secret piece of information such as responsible for the secrecy of the scheme. To protect data from malicious, intrusion and firewall cryptography as different encryption scheme.

III. PROBLEM

One problem is that in current practical systems, the encrypted data need to be decrypted before operations can be performed on them. This, furthermore, requires that the system to keep the decryption key locally. Hence, after successfully compromising a system, attackers can obtain the encryption key or monitor the system memory and CPU to successfully compromise critical data and keys.

Secure computation is a potential solution to this problem. It has been an active research area since the 1980’s. One type of secure computation algorithm, secure circuit evaluation, considers binary circuits with “and” and “negate” operations. The model involves two parties A and B, where A holds the circuit *f* and a secret *x* and B holds another secret *y*. The goal is to compute *f(x,y)* without revealing the secrets or the circuit to each other. In [Yao86], [10] Yao introduced the garbled circuit concept. In this model, B constructs the garbled circuit and sends it to A. Then B sends the encrypted inputs to A by an oblivious transfer protocol. A then evaluates the circuit and outputs the results. The goal of this approach is to allow the evaluation to be performed for the entire circuit with only a constant number of rounds of communication between the two parties. However, the message size in this algorithm increases very [11] rapidly as the circuit size grows. Also, the overhead for circuit evaluations and for oblivious transfers is excessive. In [Aba90], Abadi proposed a secure circuit evaluation protocol based on the properties of quadratic residues. In this algorithm, the evaluation of the “and” operation requires a communication message between the two parties, which makes the protocol too expensive for real world computations.

A. *Novel Analysis of Cloud computing*

Cloud comes into picture when information technology needs a way to increase the capacity on the fly without investing in new infrastructure encompasses subscription based or pay per use service. The computer John McCarthey has already predicted back in 1961 that computation may be organized as a public utility. Clouds usually do not focus on the coordination of distributed infrastructure resources that are under the control of various parties. Cloud computing mange own infrastructure that is probably more homogeneous than that of a typical grid cloud computing addresses internet scale computing problems utilizing a large pool of computing and storing resources. Computing grids were designed upon the assume the resources are dynamic heterogeneous owned by different parties while cloud computing harnesses the power of virtualization to allow users to share resources simultaneously.

Clouds computing is one of the most innovative technologies used in several companies have popped in the cloud market achieved in desired goals planned for their business expansion

B. *Cloud Follows for Use Model*

Cloud computing managed cloud services are truly cost effective, means user will have to pay only for the amount of service used by them .

C. *Availability and Performance*

When we speak about cloud the only thing that concerns us is whether such a technology can cater to the client’s needs or whether it can create a highly scalable environment. Things like cloud migration of data from one server to the cloud server etc among others are two of the activities that are catered by managed cloud service providers.

D. *Cloud Believes in Existing Resources*

suppose one of the company facing hard time in managing hardware and software, servers running extremely low and there is not enough space left for any data to be stored. To overcome such a situation cloud services are proposed so that existing servers get rest from the over loaded traffic and work environment of the company becomes more synchronized.

E. *Cost Effective:*

To enjoy in the cloud market a cost effective business environment promotes device independence the cost of hardware and software automatically cuts short although the initial expense of deploying cloud architecture is there but that also focus on pay for what we use model

IV. Commonly Used Encryption Techniques

A. *Homomorphic:*

Homomorphic cryptography is mathematics and computer science presented the first scheme in 2009 on homomorphic, the secret function evaluation private information retrieval or searchable encryption in general. Homomorphic is a encryption technology for securing cloud data to assure users of the security of information in cloud. Private cloud to its portfolio of supported environments introduced homomorphic encryption which secures one of the least aspects of cryptography. Suppose spilt key technology assured the security of data by only allowing the secret key to be derived algorithmically from the halves of the keys. A homomorphic encryption scheme allows for both addition and multiplication to be performed on encrypted data.

B. *Order Preserving Encryption*

Consider achieving OPE for multi-user systems without violating the access control policies. The multi-user OPE system includes two modules, the encryption module and the secure communication module. The DB manages two ciphers for each critical data d, one is encrypted using a classical encryption scheme, $C_{CE}(d)$, and the other is encrypted by the OPE scheme, $C_{OPE}(d)$. We use the OPE scheme Semen constructed in [Bol09] to construct $C_{OPE}(d)$, but modify it for some situations. The purpose for having two ciphers is to avoid the potential overhead in secure communication for large cipher space. The encryption module, thus, includes $C_{CE}(d)$ and $C_{OPE}(d)$.

V. Encryption is the Solution to Use in Cloud Computing

Cloud as the logical resources accessible through a computer network not from local network managing local files is hard there are security issues computer lifecycle issues access issues. Ideally easy to access the data from anywhere outsource to service provider. Authentication for cloud computing providers such as authentication transfer data securely from their servers and encrypts stored data automatically.

Besides processing computations on encrypted data, another problem is how to search on encrypted data. One type of search queries is based on exact-match. Generally, additional “indices” are stored together with the encrypted data or special structures are “embedded” into the encrypted data to facilitate the exact-match search by DBMS [Hal09, Ama07, Son00].

Deterministic public-key encryption [Bel07, Bel08, Bol08] has also been used to realize exact-match queries. Since the encryption is deterministic, DBMS can perform exact-match search directly on the encrypted data. Compared with exact-match queries, range queries are much more commonly used. In some cases, range queries can be converted to exact-match queries. However, even if it is possible, the conversion may result in too many exact-match queries. In fact, it is difficult to convert most of the range queries to exact-match queries. Various methods have been proposed to handle range queries. In [Bon07], a basic encryption scheme is introduced to support range queries such that the cipher text of a data entry d with respect to a potential query predicate p contains the information of whether d satisfies p. For each possible query predicate, there should be a corresponding cipher text. [Bon07, Shi07] actually improve the size of the cipher text in the basic scheme, but they still incur an extremely high space overhead. In [Li05] the authors use prefix-preserving encryption (PPE) [Xu02] to support range queries. PPE has the property that if two sequences have identical x prefixes, then their cipher texts also have identical x prefixes. Therefore a range query can be converted to a prefix search problem. However PPE has certain security problems [Ama07, Li05] and their data structure and query formats are too specialized to be practical [Bol09]. Another method to realize range queries is via order preserving encryption (OPE) [Beb02, Ozs03, Hac02, Agr04, Bol09]. OPE is a symmetric-key encryption scheme that preserves the order of the data defined in Definition 2.

Suppose that $SEm,n = (Km,n, Em,n, Dm,n)$ is an symmetric-key encryption scheme with the domain $[m] = \{1, \ldots, m\}$ and range $[n] = \{1, \ldots, n\}$ where $Km,n: \{0,1\}^* \rightarrow \{0,1\}^*$ is the key generation algorithm, $Em,n: [m]\times\{0,1\}^* \rightarrow [n]$ is the encryption algorithm, and $Dm,n: [n]\times\{0,1\}^* \rightarrow [m]$ is the decryption algorithm. SEm,n is an OPE scheme if $Em,n(pt, k) \leq Em,n(pt', k), \forall\ pt \leq pt'$.

Thus, range queries can be handled efficiently using conventional DBMS techniques, such as establishing the B+ tree on cipher texts. There are various constructions of OPE. In [Beb02], the proposed OPE first generates a sequence of random numbers and then, encrypts an integer x by adding x to the sum of the first x random numbers. In [Ozs03], a sequence of strictly increasing polynomial functions are used to construct the OPE. The encryption of an integer x is the outcome of the iterative operations of those functions on x. In [Hac02], the OPE is constructed by using a mapping function composed of partition and identification functions. The partition function divides the range into multiple partitions, and the identification function assigns an identifier to each partition. Then, the mapping function maps an integer x to an identifier. Since different integers may be mapped to the same identifier, the OPE may output false comparison results. In [Agr04], it assumes that there is no plaintext attack (the adversary can only view cipher text). Under this assumption, an OPE algorithm is secure if the outputs of the OPE follows a user-specified distribution. The OPE is constructed in three steps: modeling the input and target distributions as linear splines, flattening the plaintext database into a flat (uniformly distributed) database, and transforming the flat database into the cipher database. Experiments show that the outputs and the target distribution (the authors considered three distributions, including Guassian, Zipf, and uniform distributions) cannot be distinguished by Kolmogorov-Smimov test. In [Bol09], a cryptography based OPE construction approach is proposed. It defines the security of an OPE algorithm by the ideal model and the real model, and construct the OPE in the real model to satisfy the security "implied" in the idea model. In the OPE construction, a plaintext x is mapped to its cipher by a "binary-search-like" process in the cipher space with the searched points being mapped back to the plaintext space using the hyper geometric distribution. In [Xia10], we study the security of the OPE scheme constructed in [Bol09], and derive the upper bound probability for an adversary to recover the plaintext under chosen plaintext attacks.

One limitation in existing OPE schemes is that there is no consideration of users, which makes the schemes impractical. Generally, a system would deal with multiple users with different access privileges. Consider a system consisting of a server managing a database that is accessed by many users. The critical data in the database are encrypted by an OPE scheme using a master encryption key. The server should not have the knowledge of the master key. When a user sends a query to the server, critical data in the query need to be encrypted and the returned results need to be decrypted. In conventional OPE schemes, it is implicitly assumed that the user knows the master key and, hence, is able to encrypt and decrypt the corresponding data. However, in practice, giving the master key to the users is insecure. There is a significant probability for the server (or an adversary who compromises the server) to collude with one of the users and compromise the entire database. A potential solution is to use different encryption keys for different privilege domains. But it may not be easy to design an OPE to perform comparisons cross domains.

VI. Experiment Design

The proposed experiment setup considers the cloud systems sender and receiver has installed on it, the sender system is connected to access point. In the proposed setup sender system encrypts a several files for different data types data from kilobytes to megabytes for any data, encryption algorithm that are selected in the experiment are Homomorphic and Order Preserving.

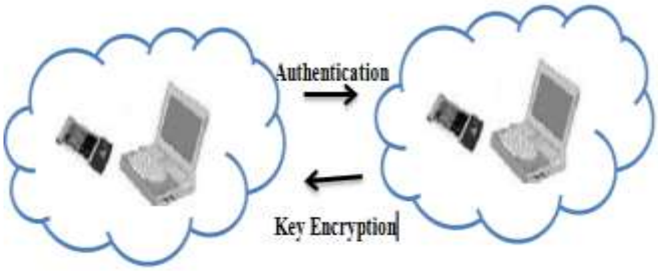


Fig. 3. Presents the Proposed Implementation

These implementations are thoroughly tested and are optimized to give the maximum performance for each algorithm that supposed to be the best encryption algorithms by a different implementations program to give the maximum performance make sure the results are the same using multiple platforms. Then for transmission of data sender and receiver systems in cloud are connected wirelessly, data is transmitted from the first sender system to receiver system through the wireless link using any protocol, the experiment are applied in two mode of wireless LANs connection. First data is transmitted using open requirement system authentication (no encryption) second method, data is transmitted using encryption key authentication. The effects of different signal to noise conditions and its effect on transmission of data under excellent signals which performance best benefits encryption time battery power and transmission time in many cases.

A. Applications of Cryptography

The aim of protecting information by hiding into an unreadable model called cipher text, only those who possess a secret key can decipher the message into plain text encrypted messages can sometimes be broken by crypt analysis called breaking of code can be virtual. Cryptographic service provider provides software and hardware based encryption and decryption services at minimum it consists of a dynamic link library that implements the functions in crypto interface.

Cryptographic algorithms are different key function such as Secret key uses one only key for encryption and decryption, Public key uses two key one for encryption and other for decryption. Hash functions have no key since plain text is not recoverable from the cipher text and Significance of key length.

1) Password Protection
2) Pretty Good Privacy
3) Secure Transaction Protocols for the World Wide Web
4) Protection of IP Protocol

VII. CONCLUSION

This research work proposed and listed in the field of cryptography in cloud computing analysis. It focuses on risk problems in cloud environment, several techniques, analysis method, experiment setup, variety of applications that are commonly used cloud analysis. Wide range of this work is efficient never implemented before. In fact it has scope of computer networks and cryptographic analysis. Finally this paper concludes encryption in cloud tasks are very innovative, future extends with machine learning algorithms which detect intrusion

REFERENCES

[1] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, Order-preserving encryption for numeric data, ACM SIGMOD International Conference on Management of Data 2004, pp. 563-574.

[2] G. Amanatidis, A. Boldyreva and A. O'Neill, Provably-secure schemes for basic query support in out- sourced databases, Working Conference on Data and Applications Security, 2007, pp. 14-30.

[3] G. Bebek. Anti-tamper database research: Inference control techniques, Technical Report EECS 433 Final Report, Case Western Reserve University, November 2002.

[4] M. Bellare, A. Boldyreva, and A. O'Neill, Deterministic and efficiently searchable encryption, CRYPTO 2007, pp. 535-552.

[5] M. Bellare, M. Fischlin, A. O'Neill, and T. Ristenpart, Deterministic encryption: Definitional equivalences and constructions without random oracles, CRYPTO 2008, pp. 360-378.

[6] A. Boldyreva, S. Fehr, and A. O'Neill, On notions of security for deterministic encryption, and efficient constructions without random oracles, CRYPTO 2008, pp. 335-359.

[7] A. Boldyreva, N. Chenette, Y. Lee, A. O'Neill, Order-preserving symmetric encryption, Eurocrypt 2009, pp. 224-241.

[8] D. Boneh and B. Waters, Conjunctive, subset, and range queries on encrypted data, TCC 2007, pp. 535-554.

[9] Daemen.J, and Rijmen.V(2001). "Rijndael: The Advanced Encryption Standard."D r.Dobb's Journal, PP. 137-139.

[10] El-Fishawy.N(2007)," Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms", International Journal of Network Security, PP.241–251.

[11] Endey .J, Arbaugh .W.A(2003), "Real 802.11 Security: Wi-Fi protected access and 802.11i," Addison Wesley.

[12] Fischer.K(2004),. "Embedded wi-fi market undergoing major shift," Web article, 23 Aug.

[13] Gary C. Kessler, Ph.D., CCE, CISSP, is the president and janitor of Gary Kessler Associates, an independent consulting and training firm specializing in computer and network security, computer forensics, Internet access issues, and TCP/IP networking.

[14] Armbrust, Michael, Armando Fox, Rean Griffith, et al. 2009. Above the Clouds: A Berkeley View of Cloud Computing. Berkeley: EECS Department, University of California.

[15] Babbage, Charles. 1864. *Passages from the life of a philosopher*. London,: Longman, Green, Longman, Roberts, & Green.

[16] Balan, RK, M Satyanarayanan, SY Park, et al. 2003. Tactics-based remote execution for mobile computing. Paper read at International Conference On Mobile Systems, Applications And Services, at San Francisco, California.

About Author (s):

[Cryptographic service provider provides software and hardware based encryption and decryption services at minimum it consists of a dynamic link library that implements the functions in crypto interface.]

[The aim of protecting information by hiding into an unreadable model called cipher text, only those who possess a secret key can decipher the message into plain text encrypted messages can sometimes be broken by crypt analysis called breaking of code can be virtual.]

[Cryptographic algorithms are different key function such as Secret key uses one only key for encryption and decryption, Public key uses two key one for encryption and other for decryption.]