Use of Diffie Hellman Key Exchange for Information Transmission and File Integrity Monitoring in Cloud

Shweta Sharma
Assistant Professor
Department of Computer
Science & Engineering
DIT University
Dehradun,India

ABSTRACT
In today's computing era,there has arisen an immense requirement for secure and trusted security frameworks/models in cloud computing.These models allow the cloud service provider to establish a trusted bond among clients,which is the prime requisite for cloud e-businesses nowadays. Keeping this orientation in mind,we have proposed a comprehensive security framework which provides extra layer of security to the information transmitted among client and server ends & also sustains the information integrity at both terminals.It provides the data security during storage at cloud server . This incorporates confidentiality,authentication and integrity of the involved information among client-server terminals.Numerous cryptographic algorithms have been used to apply in the implemented tool. Diffie- Hellman key exchange scheme has been applied in this research work.

General Terms
Cloud Computing, Information Security,Cloud Server.

Keywords
Deffie Hellman Key exchange, Information Integrity,Hash Algorithms.

1. INTRODUCTION
In Cloud Computing,various information related security issues have been diagnosed and researched upon.In terms of information confidentiality,weakness in cryptographic algorithms leads to vulnerable security risks for information stored at cloud server[2].Along with this,client data redundancy leads to data loss and so,there exists an immediate requirement for information integrity and availability to the client to maintain bussiness trust levels among client and cloud sever[4]. The above marked portion has been studied and an approach has been proposed to vanish such issues.Many security concerns/factors have been found out in our analysis.As per statistics shared in the following diagram, 10% reports for security issues had been related to the data security only.It proves the immense need of research work to bring solutions to this research issue[5].We have worked and proposed tool based on the secure storage of client data in cloud server.The outside/thwart attacks must be prevented and handled to inculcate cloud based business.Various other issues related to compliance,governance,legal issues ,network security and interfaces etc have also been reported and must be worked upon in future researches as well[3][6].

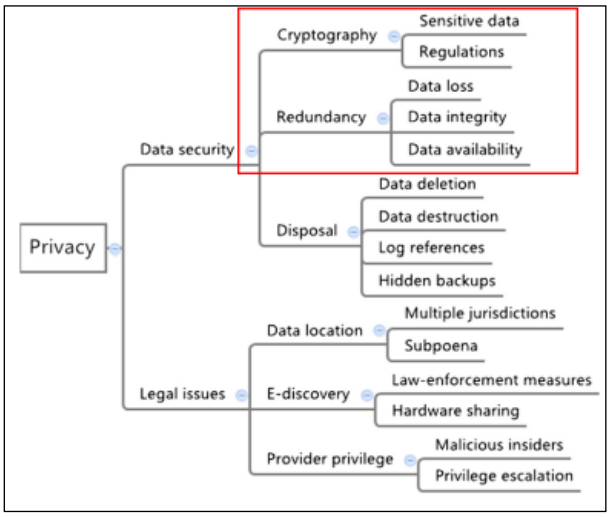

Figure 1: Data Security Issues in Cloud Computing [1]

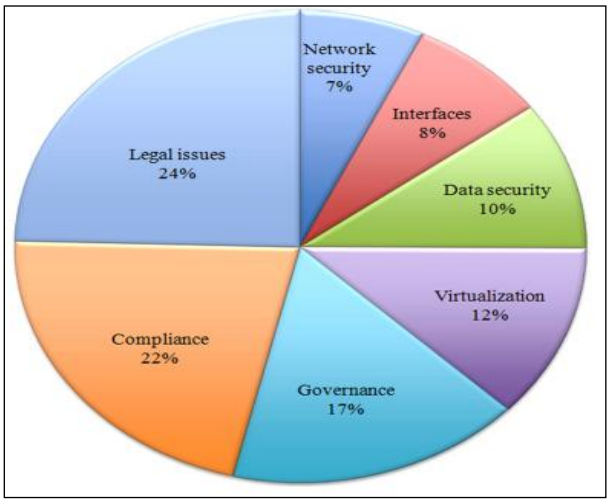

Figure 2: Pie Chart for Security Concerns [3]

2. RELATED WORK
As per our research survey,a significant amount of research work has already been conducted in this direction.Various tools and frameworks have been designed and implemented as well.Following table provides the details of tools developed and their features:-

Table 1:Prior implemented tools and their features

TOOLS DEVELOPED	CHARACTERISTICS
VM Fence[11] proposed by Hai Jin et al	Monitors network flow and integrity in real time.
Storage-based IDS propose by Pennington et al. [12]	Allows the storage systems to watch for data modification.
I3FS[13]	Intercepts file system calls and injects its integrity checking operations in kernel mode.
Xen FITs[14]	Monitored system consists of breakpoints that intercept file system calls. E.g. open, close, write.
Flogger[15]	File centric logger for monitoring file access and transfers within cloud.
Tripwire[16]	A Host based IDS that alerts on macro changes to the files and folders.

They monitor network flow through cloud infrastructure as various clients could connect to cloud server through virtual machines(VMs).Various network based attacks may occuron server. There is an immense requirement for light weight tools which could provide integrity checks over stored data[17][18]. We analyzed that for cloud computing, there is a requirement for a light weight, efficient, low operational cost and secure optimized solution. In tools such as file integrity loggers, there exists an immense database availability which could be an overhead to the cloud server memory utilization functions.Following tool had been implemented and proposed to provide file integrity monitoring and establishment by cloud server [19][20].

DRAWBACKS: There were few drawbacks shortlisted for this model[8][9]:-

i. Lack of transparency between client and server entities.
ii. The client is not directly involved in the hash checksum computation process required for integrity maintenance on server.

iii. Attacker could be in form of server only.

iv. Lack of trust establishment between involved entities.
v. Absence of proper formulated key ecxhange mechanism required for key transfer between client and server entities.

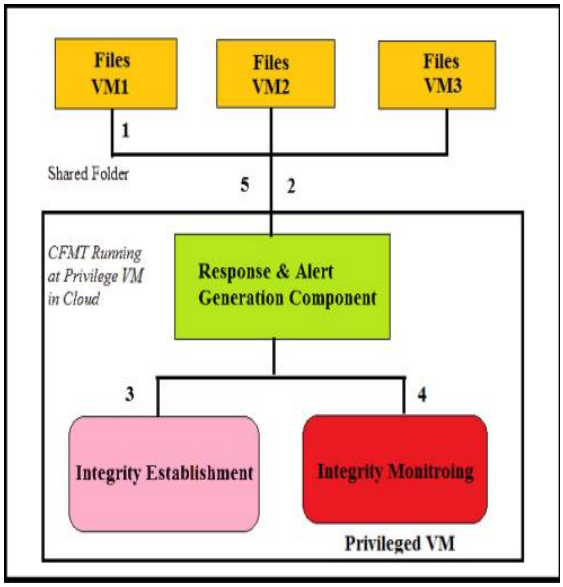

Figure 3: Architecture of CFMT (Cloud File Monitoring Tool) [8].

3. PROPOSED RESEARCH WORK

In order to provide a light weight and time/cost efficient tool for information integrity establishment and maintenance ,we have proposed the model.Following are the sequence of steps to be executed in cloud server- client scenario(where the client wishes to store its information on cloud server in form of a file record):-

i. Firstly, the client registers itself with cloud server.Then, the server authenticates the client using Identity based authentication scheme[7][8].

ii. The client stores its file record on the server hard disk by proper access channels as provided by cloud server.

iii. Now, the server creates a backup replica for client's file (as a backup management activity)and stores it in a secret folder on its drive.

iv. The checksum computation process gets started and the server calculates the hash of the information stored in client's file.

v. The secret key gets finalized using Diffie- Hellman key exchange process and the computed hash gets encrypted by server using the secret key.It is being sent to the client terminal.

vi. The client decrypts the packet using secret key and apply nonce and hash algorithm and finally implement the RSA digital signature using its private key and stores the final checksum on the cloud server(to be stored between hash tags within the file only).

vi. Whenever,the client desires to locate its file on server,the server recomputes the final checksum value using client's invloved as discussed earlier and verifies if the stored and recomputed hash tags are same or not.

vii. If they are same,it indicates the stored file is intact and can be shared with client.If not,then there exists a security breach and the back up replica of the file will be provided to theclient

and new hash tags will be recomputed and stored in file(under cloud platform).

ALGORITHM:-
The process algorithm for proposed tool has been stated as below:-
a.Initialize cloud server process be CS and client process be CL.CS establishes the connection with CL and session activates.
b.CS authenticates CL using Identity based authentication scheme[].

c.CS uploads given input file F in shared folder located at server's hard disk drive.

d.Integrity Establishment Process:
begin
CS apply SHA algorithm on F .
Add random number Nonce N on above.

CS and CL applies Diffie Hellman key exchange algorithm to finalize a common secret key(K) .

Checksum gets encrypted using common secret key K by CS and send to CL .
CL decrypts the same and append Nonce N'and apply SHA to produce hash product H.

CS apply RSA digital Signature scheme(using CL private key) on H.

Send the finalized checksum(FC) back to CS for further storage.
CS saves FC as secure tags<>inside input file F.
end
e.Integrity Monitoring Process(called by CS/CL):
begin
CS recomputes FC' using Integrity Establishment process in session with CL.
If(FC'==FC)
Say-File Intact.Integrity Sustained.
ElseSay-File Not Intact.File modified

Replace F with Backup replica.

Call Integrity Establishment process.

End.

4. RESULTS & CONCLUSION

The proposed scheme had been applied in windows7 and have used Linux based Oracle VM virtual box(software).This utility provides a virtual client- server environment on physical machine. Using this,we have developed a client-server like environment and implemented the proposed architecture and algorithmic steps.Following screenshots shows the executed operations.As per our computations,it has been observed that the proposed model provides significant client-server communications and alleviates the trust paartnershsip among involved entities while information exchange in cloud computing.This tool also proves to be time and cost efficient as it computes the integrity establishment and monitoring in seconds for a few byte

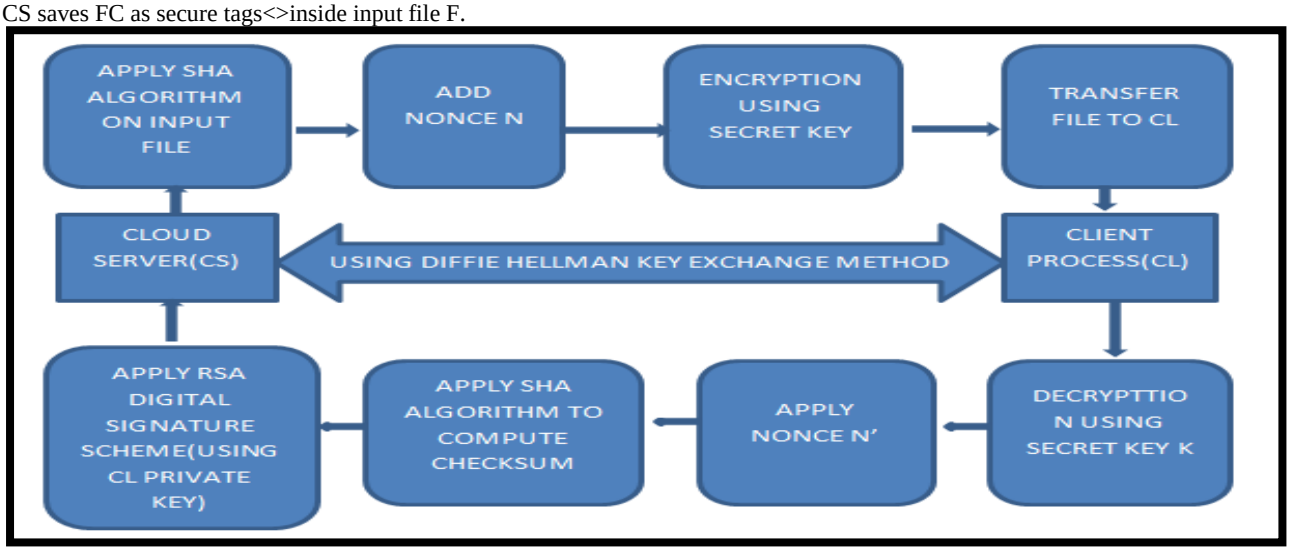

Figure 3:Schematic Representation of proposed Information Integrity Maintenance in Cloud(using Diffie Hellman Key Exchange method)[10].

sized file (in comparison with long server overhead delays) and requires no database support to function.And thus, proves to be an efficient technique for information transmission and integrity sustainance over cloud platform.Diffie –Hellman key exchange enhances the security level during information exchange among client-server systems.

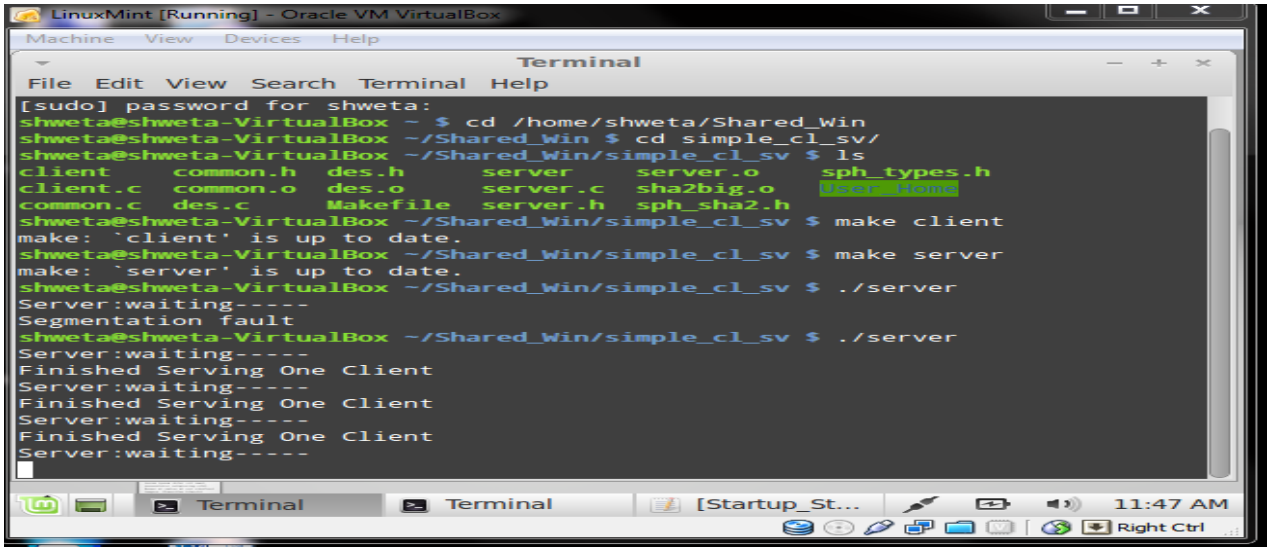

Figure 4: Screenshot of Server Process during Initialization mode.

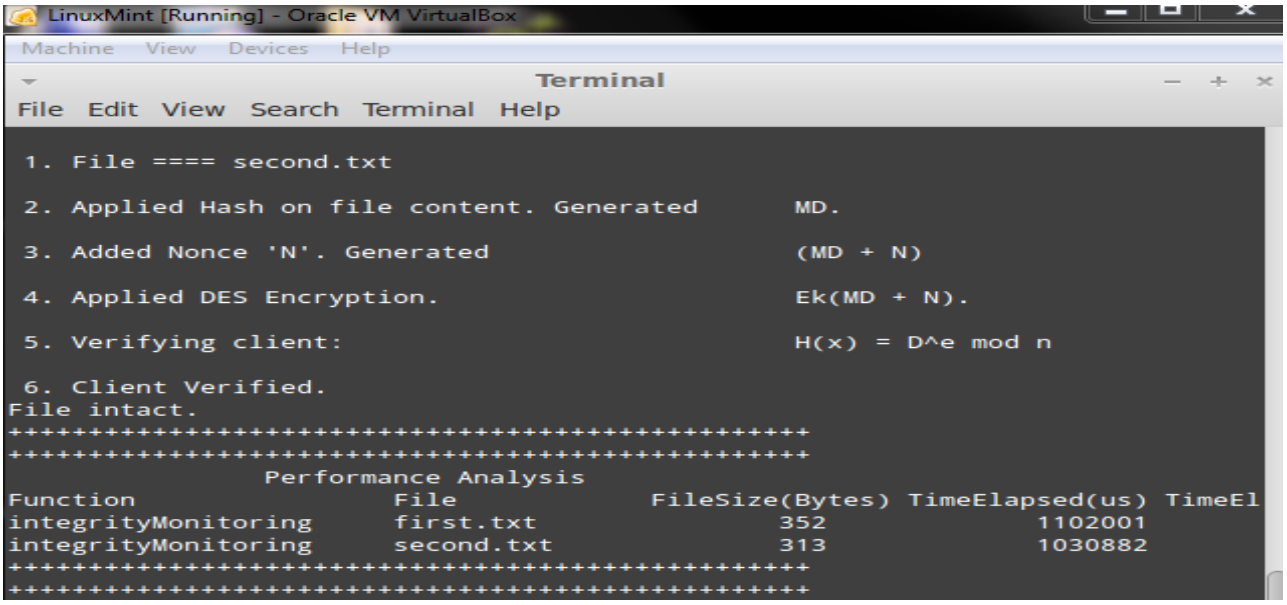

Figure 5: Screenshot of file restoration functionality on any kind of client information modification within server.

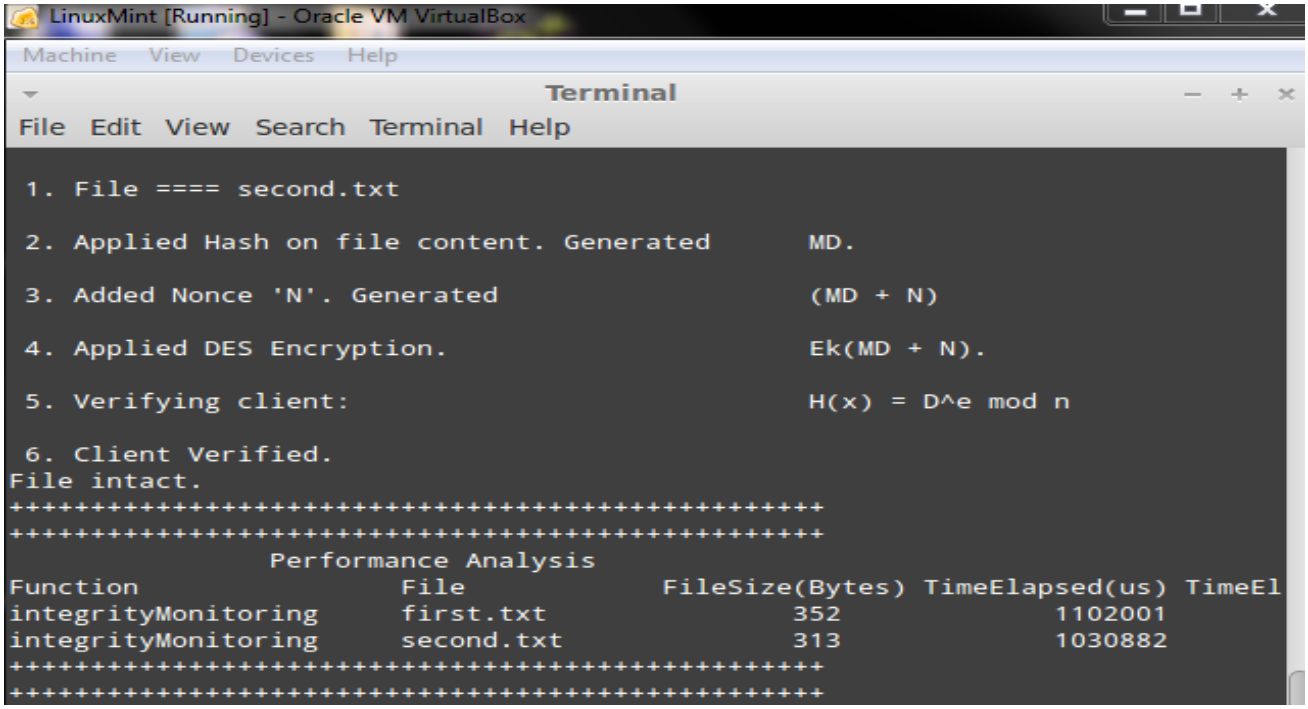

Figure 6: Screenshot of Performance Analysis (Time consumed during Integrity Maintenance) for a given file.

5. REFERENCES

[1] G A Solanki, "Welcome to the Future of Computing: Cloud Computing and Legal Issues", International Journal of Scientific & Technology Research 2012, vol1, issue 9.

[2] Jian Wang, Yan Zhao, Shuo Jiang, Jiajin Le, "Providing Privacy Preserving in Cloud Computing" 2010, IEEE.

[3] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, Makan Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing", Gonzalez et al. Journal of Cloud Computing: Advances, Systems and Applications 2012.

[4] Lijun Mei, W .K .Chan, T .H .Tse, "A Tale of Clouds: Paradigm comparisons and some thoughts on research issues", 2008 IEEE Asia-Pacific Services Computing Conference.

[5] Balachandra Reddy Kandukuri, Ramakrishna Paturi V, Dr. Atanu Rakshit, "Cloud security Issues"2009, IEEE.

[6] M. Sudha, M. Monika, "Enhanced Security Framework to Ensure Data Security in Cloud Computing Using Cryptography", Advances in Computer Science and its Applications 32 Vol. 1, No. 1, March 2012, Copyright © World Science Publisher, United States. www.worldsciencepublisher.org.

[7] Hongwei Li, Yuanshun Dai, Ling Tian and Haomiao Yang, "Identity-Based Authentication for Cloud Computing", Springer - Verlag Berlin Heidelberg 2009.

[8] Sanchika Gupta, Anjali Sardana, Padam Kumar, "A light Weight Centralized File Monitoring Approach for Securing Files in Cloud Environment ",The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012) ©IEEE 2012.

[9] Sanchika Gupta, Anjali Sardana, Padam Kumar , Ajith Abraham, "A secure and light weight approach for critical data security in cloud", 2012 Fourth International Conference on Computational Aspects of Social Networks (CA Sons).

[10] Forouzan, "Cryptography and Network Security", TMH 2012.

[11] A.H. Steven, F. Stephanie and S. Anil, "Intrusion detection using sequences of system calls," J Compul. Secure. Vol. 6, no. 3, 1998, pp. 151-180.

[12] G. P. Adam, D. S. John, G. John Linwood, A. N. S. Craig, R. G. Garth and R. G. Gregory, "Storage-based intrusion detection: watching storage activity for suspicious behavior," Book Storage-based intrusion detection: watching storage activity for suspicious behavior, Series Storage-based intrusion detection: watching storage activity for suspicious behavior, ed., Editor ed/'eds., USENIX Association, 2003.

[13] S. Patil, A. Kashyap, G. Sivathanu and E. Zadok, "13FS: An in-kernel integrity checker and intrusion detection file system."

[14] Q. Nguyen Anh and T. Yoshiyasu,"A novel approach for a file-system integrity monitor tool of Xen virtual machine," Book A novel approach for a file-system integrity monitor tool of Xen virtual machine, Series A novel approach for a file-system integrity monitor tool of Xen virtual machine, ed.,Editor ed.ls\eds., ACM, 2007.

[15] R.K.L. Ko, P. Jagadpramana and L. Bu Sung, "Flogger: A File-Centric Logger for Monitoring File Access and Transfers within Cloud Computing Environments," Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on , pp. 765-771.

[16] H. K. Gene and H. S. Eugene, "The design and implementation of tripwire: a file system integrity checker,"BookThedesignandimplementationoftripwire:ai le system integrity checker, Series The design and implementation of tripwire: a file system integrity checker, ed., Editors, ACM, 1994.

[17] Meiko Jensen, Jorg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On technical security issues in cloud computing" 2009, IEEE Computer Society.

[18] Henry Kasim, Terence Hung, Xiaorong Li, "Data Value Chain as a Service Framework: for Enabling Data Handling, Data Security and Data Analysis in the Cloud", 2012 IEEE 18th International Conference on Parallel and Distributed Systems.

[19] Tina Francis, S. Vadivel, "Cloud Computing Security: Concerns, Strategies and Best Practices: Proceedings of 2012 1ntemational of Cloud Computing, Technologies, Applications & Management", 2012 IEEE.

[20] G A Solanki, "Welcome to the Future of Computing: Cloud Computing and Legal Issues", International Journal of Scientific & Technology Research 2012, vol1, issue 9.