International Journal of Security and Its Applications
Vol. 12, No. 6 (2018), pp.37-46
http://dx.doi.org/10.14257/ijsia.2018.12.6.04

Space and Security Issues in Cloud Computing: A Review

Debnath Bhattacharyya

Department of Computer Science and Engineering,
Vignan's Institute of Information Technology,
Visakhapatnam-530049, AP, India
debnathb@gmail.com

Abstract

Cloud computing is the most advanced and mostly used technology for the never-ending IT and software industries. Various numbers of large servers were used in the cloud models for storing the vast amount of data. To store massive databases, various setoff servers with high-end hardware and with fast internet facilities were required and with these set of servers for providing services to the end users.In these servers, users store massive amount of data and also retrieve from time to time, providing security to the data in these cloud computing models was very much essential and important. Hence, as the data storing in the various locations of the servers, the provision of adjusting the various amount of considerable data in the servers at various locations from time to time is essential and also the provision of security to these massive set of databases and also retrieving and storing the data is more critical. Hence, we need to provide more security to the data being stored in the huge number of the server. As we need to provide security to these servers, several factors are important to note. In this paper we present the detail description about these points.

Keywords: *Security techniques, space issues for security, architecture, cloud computing, firewalls.*

1. Introduction

Cloud computing is the software platform for providing and delivery of various computer services like storage, server spaces, software's and analytics over the internet to offer faster and innovative facilities to the end users. For using these services, the users need to pay very less or nominal fees such that they can enjoy various advanced benefits in terms of technology and the gadgets you can use from the help from these networks. Traditional applications before to the introduction of cloud models, the applications cost was very high and the operating costs were high and also the utility of the public in misuse mode was very high. Hence, the introduction of cloud models has given the users with good quality of services with good technologies at lower costs.

By using the cloud related services, several advantages are being provided to the end users. Some of them are the cost of the equipment. By the usage of cloud computing technology, the customers no need to purchase the more cost effective hardware and its related units. With the service from the cloud managed service provider will provide such high end, very fast hardware requirements will be met by the customers. The purchasing cost of such huge servers and maintenance costs were reduced a lot to the customers. Not only these benefits, but also other benefits like the power benefits, hardware purchase and maintenance costs like the maintenance of data centers where huge servers can be placed are the other benefits. The operating speed of these networks are at high speeds as the number of customers using these services are in known number and the adjustment of

Received (August 5, 2018), Review Result (October 11, 2018), Accepted (October 21, 2018)

ISSN: 1738-9976 IJSIA

bandwidth for providing such number customers is very easy and easy to maintain. The services can be provided to any type of customers from small scale industries to large scale industries and from normal people to the highly reputed people ion the society.

The security for the data to be storing in these networks was high as it was a paid and use service. Still, so many people try to grab the system and misuse it or some people or users tries to spoil the system. Hence, providing security to the data in these sorts of network is very difficult and also more important. Similarly, we need to study the challenges and various issues that might be considered as important while we are working on these networks. Storing data in these cloud based data centers is also an important and very interesting issue to be considered. The architecture of a cloud computing models is as follows,

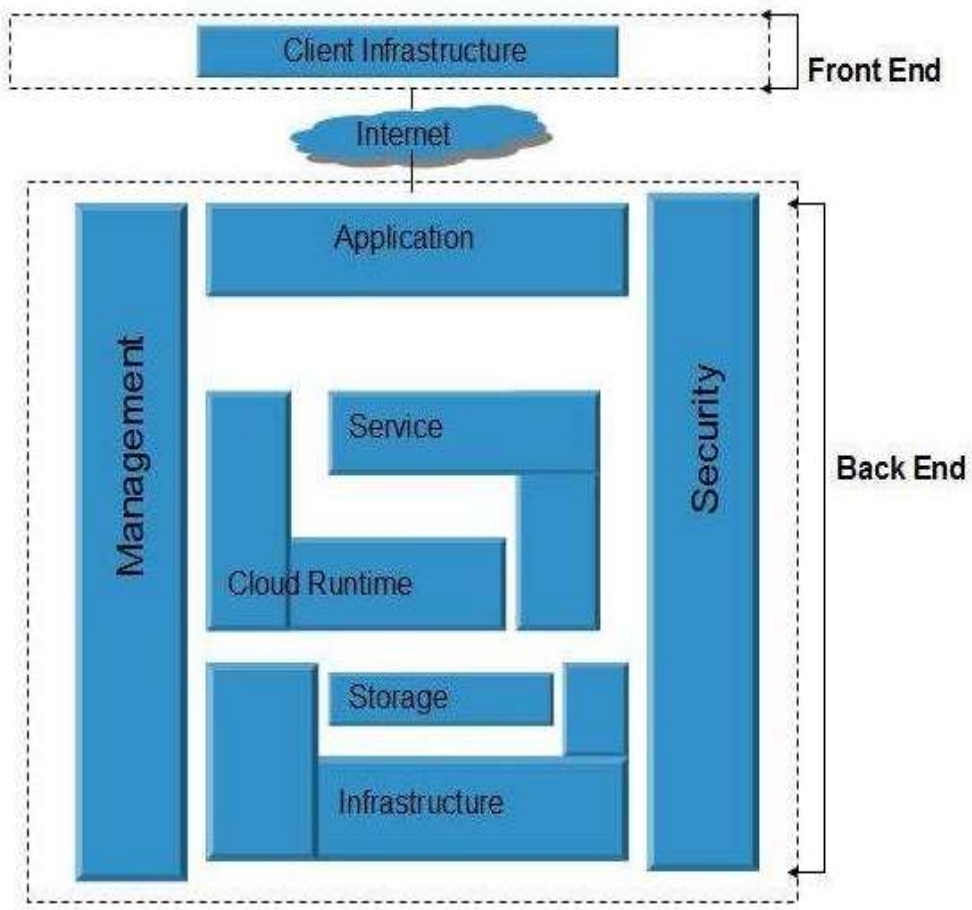

Figure 1. Cloud Computing Architecture

2. Cloud Storage Models

Cloud storage is one of the service model provided by the cloud computing environment which helps the users or the people who are maintaining these cloud related operations by means of data maintenance, backing up of data remotely. Also this model helps in making the current backed up data be available to all the people who are staying remote places and other accessible places on the earth. Wherever the internet facility is available, there you can access these services without any problems. The users who ever using the services from these cloud models, they can use these services by paying money to the service providers by pay to application or by paying the monthly bill at a time. As the technology is being increasing and developing from day to day life, the services

provided by these networks will have good services and options for the users to get from the service providers. As the technology is being increasing from day to day and new features are being incorporating into the cloud services, two problems are still making a thought for all the customers and the administrating people. Those two constraints are the security for the data to be stored in the cloud and the form of data being stored in cloud services or in other words it can be taken as the space in the cloud databases issues that were arising from day to day life usage of the various number of huge servers.

The main problem to be addressed or to be concerned in the cloud based architectures or the cloud based applications was the storage space. In general, three types of storage processes were used in cloud based applications. They are public storage, private storage and third one is the hybrid storage of data. In the public cloud storage, several services will be provided for the unstructured data. The data to be stored is stored at various locations and at various data centers those were located globally at various countries or centers with the capacity of storing at multiple areas or at multiple levels of continents. Several companies are pioneer in this business by u sing and providing services. Amazon Simple Storage Service (S3) is the leading service provider in this domain worldwide. The other set of providers in this mode are Amazon Glacier, Google cloud storage and Microsoft Azure.

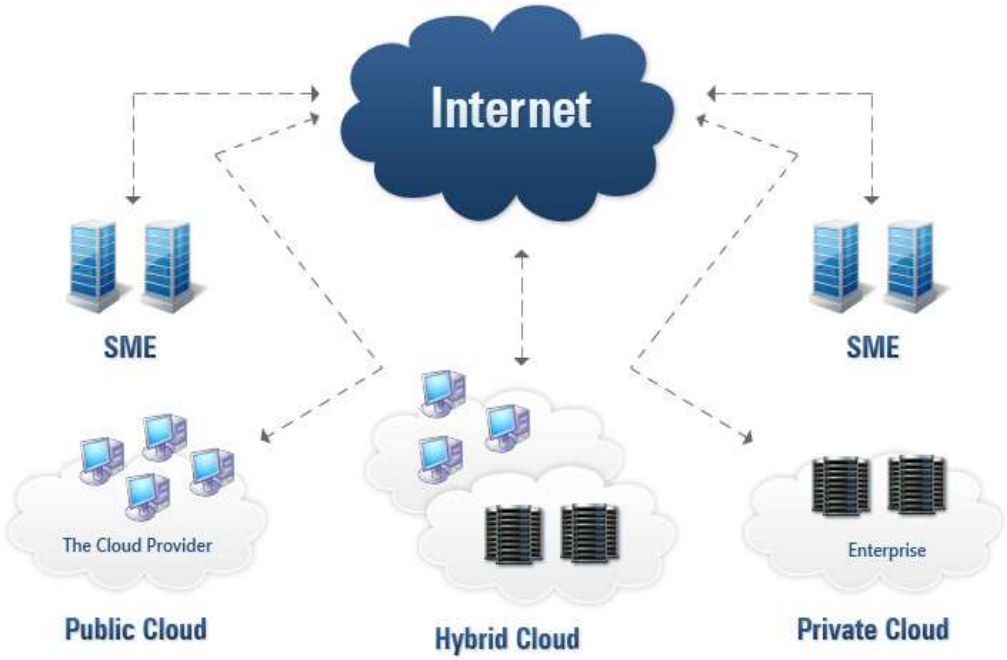

Figure 2. Various Cloud Storage Models

The other set of storage model is the private cloud storage. This sort of clouds were being developed and maintained by the organizations or private companies on their own at their premises by providing their own security by keeping their own firewalls. These clouds were developed maintained by the companies for their own data and also the companies will have more control over the data that was being stored on the cloud.

Hybrid cloud is a mix of private cloud and third-party public cloud services with orchestration between the platforms for management. The model offers businesses flexibility and more data deployment options. An organization might, for example, store actively used and structured data in an on-premises cloud, and unstructured and archival data in a public cloud. In recent years, a greater number of customers have adopted the hybrid cloud model. Despite its benefits, a hybrid cloud presents technical, business and management challenges. For example, private workloads must access and interact with

public cloud storage providers, so compatibility and solid network connectivity are very important factors. An enterprise-level cloud storage system should be scalable to suit current needs, accessible from anywhere and application-agnostic.

3. Safety and Security Issues of Cloud Storage Space

Storage organization of customers to the information in blurs and furthermore to make use of the open request with no pressure data accumulating kept up. Despite the way that cloud provider’s benefits organization and surrenders the balance of customer's data with cloud data rightness. The information proprietors having a large measure of outsourced information and analyzing the information rightness in a dim circumstance can be troublesome and expensive for data proprietors. The planned setup furthermore holds up a safe and successful quick process on subcontract information counting piece alteration, removal and join.

Perfect structures with information accumulating which need no attempt is getting more noteworthy commonness for a human being. While these electronic online associations do give goliath measures of storage room and adaptable enrolling assets, this figuring stage is shedding the dedication of neighborhood machines for information reinforce in the interim. In this way, clients are vulnerable before their cloud specialist relationship for the accessibility and dependability of their information. Late downtime of Amazon's S3[16] is such a delineation. A safe and successful storing tradition is planned that assures the information accumulating mystery and trustworthiness. The current tradition is envisioned by using the advancement of elliptic twist cryptography and quiet gathering is employed to insist the information honesty.

The strategy of access and store little records with the ability to help benefits extensively. Hadoop scattered archive structure server reasons are investigated for little record bother neighborhood. Weight on Nane Node of HADOOP flowed record structure is maintained by large measure of little archives, for data course of action amendment are not considered perfecting part is not in like manner presented. With a particular true objective to vanquish these little size issues, projected an advance that these little size issue projected a move toward. That improves the little archive capability on Hadoop appropriated record structure, in a generous gathering, an enormous number of servers both host notably joined limit and execute customer application undertaking. The purchasing cost of such huge servers and maintenance costs were reduced a lot to the customers. Not only these benefits, but also other benefits like the power benefits, hardware purchase and maintenance costs like the maintenance of data centers where huge servers can be placed are the other benefits. The operating speed of these networks are at high speeds as the number of customers using these services are in known number and the adjustment of bandwidth for providing such number customers is very easy and easy to maintain.

Characteristic	Description
Manageability	The ability to manage a system with minimal resources
Access method	Protocol through which cloud storage is exposed
Multi-tenancy	Support for multiple users (or tenants)
Scalability	Ability to scale to meet higher demands or load in a graceful manner
Data availability	Measure of a system's uptime
Control	Ability to control a system—in particular, to configure for cost, performance, or other characteristics

Figure 1. Characteristics of Cloud Storage

The most part observed of these sorts are paying little mind to the way which relies on the old convention. All these APIs are related to working up requests for advantage by procedures for the Internet. REST is a thought everything considered clears as an approach to managing administer "quality" adaptable API design. A champion among the most basic features of REST is that it is a "stateless" laying out. This suggests everything expected that would complete the request quite far cloud is contained in the request, with the objective that a sitting flanked by the requestor and the negation tip cloud is not required. It is fundamental in light of how the Internet is out and out inert (it has a different response time, and it is all things considered not snappy when risen out of a zone is an approach that has a high proclivity to the way the Internet works. Standard annual hoarding access techniques that utilisation NFS (arrange records structure) or CIFS (Common Internet File System)[17] don't work over the Internet, because of inaction.

Appropriated aggregating is for reports, which, some induce as articles. While these electronic online affiliations do give goliath measures of storage space and versatile enlisting resources, this figuring stage move, in any case, is shedding the devotion of neighborhood machines for data strengthen in the meantime. Like this, customers are defenseless before their cloud pro relationship for the availability and reliability of their data. Late downtime of Amazon's S3[18] is such a depiction. An ensured and effective putting away custom is arranged that confirmation the data collecting riddle and reliability. The other kind of data is the piece or managed data. Passed on storing up isn't for this use case. Display day Design Center (IDC) watches that around 70% of the machine set gone information on the earth is amorphous, and this is in like the way the snappiest making information altogether.

4. System and Internet Security

The broadening arrangement trade speed and hard so far flexible structure affiliations affect it still imaginable that clients to would now have the ability to buy in mind-blowing associations from data and programming that harp exclusively on remote server ranch [4]. While these electronic online associations do give goliath measures of storage room and adaptable enrolling assets, this figuring stage move, notwithstanding, is shedding the dedication of neighbourhood machines for information reinforce in the interim. In this

way, clients are vulnerable before their cloud specialist relationship for the accessibility and dependability of their information. Late downtime of Amazon's S3[4] is such a delineation. Framework security incorporates the endorsement of access to data in a framework, which is controlled by the framework chief.

4.1. Remote Network Security

Remote security is the repugnance of unapproved access or damage to PCs using remote frameworks. WEP is a broadly delicate security standard. The mystery key it uses can consistently be part instantly with a basic workstation telephone extensively open programming instruments. One prominent approach acknowledges that the PDA executes TLS over TCP/IP and the remote framework reinforces trade of IP bundles. The WAP designing is planned to adjust to the two principal limitations of remote Web get to the obstructions of the small centre (little screen assess, confined data capacity) and the low data rates of remotely automated frameworks.

5. Cryptography Mechanism

Cryptography is a methodology for securing and transmitting data in a particular shape with the objective that those for whom it is normal can read and process it. The broadening arrangement trade speed and hard so far flexible structure affiliations affect it still imaginable that clients to would now have the ability to buy in mind-blowing associations from data and programming that harp exclusively on remote server ranch [9]. While these electronic online associations do give goliath measures of storage room and adaptable enrolling assets, this figuring stage move, notwithstanding, is shedding the dedication of neighbourhood machines for information reinforce in the interim.

5.1. Riddle Key Cryptography.

The same plaintext square will reliably encode to the same cypher text while using a comparable key in a piece figure while the same plaintext will scramble to different cypher text in a stream figure. Square figures can work in one of a couple of modes; the going with four are the most basic.

• Electronic Codebook (ECB) mode is the minimum unpredictable, most obvious application: the secret key is used to scramble the plaintext square to shape a cypher text piece. Two indistinct plaintext squares, by then, will continuously deliver the same cypher text piece. Disregarding the way this is the most common Crucial secret cryptography designs are generally orchestrated as being either stream figures or piece figures. A piece figure is gathered in light of the way that the arrangement scrambles one square of data at any given minute using a comparable key on each piece. With everything taken into account, the same plaintext piece will reliably encode to the same ciphertext while using a comparable key in a square figure while the same plaintext will scramble to different cypher text in a stream figure. Square figures can work in one of a couple of modes; the going with four is the most fundamental.

6. Firewalls

A firewall outlines a deterrent through which the movement going toward each way should pass. A firewall security approach oversees which action is affirmed to go toward each way. Firewalls compel repressions on drawing closer and dynamic Network packs to and from private frameworks. Drawing nearer or dynamic development must experience the firewall; simply affirmed development is allowed to experience it. Firewalls make checkpoints between an inside private framework and general society Internet, generally called smother focuses (acquired from the vague military term of a fight confining

geographical component). Firewalls can make choke centres in light of IP source and TCP port number. They can in like manner fill in as the phase for IPsec. Using tunnel mode capacity, the firewall can be used to complete VPNs. Firewalls can in like manner bind sort out the presentation by covering the internal framework structure and information from individuals as a rule Internet.

6.1. Package Filter

A package channel is a different firewall that techniques organize development on a package-by-package introduces. Its rule work is to channel development from a remote IP have, so a change is relied upon to interface the inside framework to the Internet. The switch is known as a screening switch, which screens packages leaving and entering the framework. Since distribute firewalls don't take a gander at upper-layer data, they cannot turn away ambushes that use application-specific vulnerabilities or limits. Package channel firewalls are all things considered defenseless against strikes and try that adventure issues inside the TCP/IP detail and tradition stack, for instance, organize layer address spoofing. Various package channel firewalls cannot perceive a framework package in which the OSI Layer 3 watching out for information has been adjusted. Mocking strikes are all around used by interlopers to avoid the security controls executed in a firewall arrange.

6.2. Stateful Packet Inspection

A Stateful package examination firewall reviews unclear package information from a bundle filtering firewall, yet what's more records information about TCP affiliations. Some Stateful firewalls moreover screen TCP gathering numbers to maintain a strategic distance from attacks that depend upon the game plan number, for instance, session holding. Some even analyses confined measures of usage data for some unusual traditions like FTP, IM and SIPS charges, remembering the real objective to recognize and track related affiliations.

7. Conclusion

The information storing in the cloud is additional painful than standard limit since of its accessibility, versatility, execution, convenience and its useful necessities. With the delicate advancement in the Internet, framework and data security have transformed into unpreventable stress for any affiliation whose inward own framework is related to the Internet. The security for the data has ended up being significantly crucial. Customer's data security is a central request over the cloud. This paper rapidly displays the possibility of security issues and storing issues, based on the perils of PC compose security and work ought to be conceivable on crucial scattering and organization. The authors mainly based on data amassing points that cloud master associations are pursuing to hoard the information and safety standpoint to be obliged that information set away in dim. We explored Amazon s3 [4] and outcast looking at frameworks which are used for information build up and safety for information in dim.The authors had discussed about the basics of cloud computing, applications and advantages of cloud computing and other advantages for the common users also had discussed. The architecture of the cloud computing model was discussed in detail and the various types of data storage models were discussed in detail. Several problems and issues that affect the performance of the cloud models were also discussed in detail.

References

[1] Karan Singh et.al. A review paper on network security, International journal of computer science and security, Vol.1, No.1. Pp.52-69.
[2] Shyam Nandan Kumar, “Technique for Security of Multimedia using Neural Network,” Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014
[3] Simmonds, A; Sandilands, P; van Ekert, L (2004). Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317-323.
[4] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". Introduction to Modern Cryptography. p. 10.
[5] Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. “A. Handbook of Applied Cryptography”. ISBN 0-8493-8523-7.
[6] https://www.tutorialspoint.com/cloud_computing/cloud_computing_architecture.htm [Last Accessed on -7-10-2018].
[7] Davis, R., “The Data Encryption Standard in Perspective,” Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.
[8] S. NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004.
[9] Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg, March 2001.
[10] https://www.google.co.in/search?q=private+cloud+model&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiWutzrivTdAhVOaCsKHWCwA1EQ_AUIDigB&biw=1366&bih=657#imgrc=p7Q7FYqw3qbJtM: [Accessed on 07-10-2018].
[11] FIPS 197,Advanced Encryption Standard, Federal Information Processing Standard, NIST, U.S. Dept. of Commerce, November 26, 2001.
[12] Bruce Schneier (1993). "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)". Fast Software Encryption, Cambridge Security Workshop Proceedings (Springer-Verlag): 191-204.
[13] Schneier, Bruce (2005-11-23). "Twofish Cryptanalysis Rumors". Schneier on Security blog. Retrieved 2013-01-14.
[14] Matsui, Mitsuru; Tokita, Toshio (Dec 2000). "MISTY, KASUMI and Camellia Cipher Algorithm Development". Mitsibishi Electric Advance (Mitsibishi Electric corp.) 100: 2-8. ISSN 1345-3041.
[15] General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms". 3GPP. 2009
[16] O. Dunkelman, N. Keller, A. Shamir, \A practical-time attack on the KASUMI cryptosystem used in GSM and 3G telephony," Advances in Cryptology, Proceedings Crypto'10, LNCS, T. Rabin, Ed., Springer, Heidelberg, 2010
[17] R.L.Rivest, A.Shamir, and L.Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communication of the ACM, Volume 21 No. 2, Feb. 1978.
[18] Diffie, W.; Hellman, M. (1976). "New directions in cryptography". IEEE Transactions on Information Theory 22 (6): 644-654.
[19] Koblitz, N., 1987. “Elliptic curve cryptosystems. Mathematics of Computation” 48, 203-209.
[20] Miller, V., 1985. “Use of elliptic curves in cryptography”. CRYPTO 85.
[21] FIPS 180, Secure Hash Standard, Federal Information Processing Standard (FIPS), Publication 180, NIST, U.S. Dept. of Commerce, May 11, 1993.
[22] R. Shiva Kumaran, Rama Shankar Yadav, Karan Singh ”Multihop wireless LAN ” HIT haldia, March 2007.
[23] S. Holeman, G. Manimaran, J. Davis, A. Chakrabarti, Differentially secure multicasting and itsimplementation methods, Computers & Security Vol 21, No 8, pp736-749, 2002.
[24] S.M. Bellovin, M. Leech, and T. Taylor. ICMP Traceback Messages. Internet draft: draftietfitrace03.txt, January 2003.
[25] Seung Yi, Prasad Naldurg, Robin Kravets, “A Security-Aware Routing Protocol for WirelessAd Hoc Networks” IEEE 2003.
[26] M. Bechler, H.-J. Hof, D. Kraft, F. Pählke, L. Wolf, “A Cluster-Based Security Architecture forAd Hoc Networks” IEEE INFOCOM 2004.
[27] Mike Just_ EvangelosKranakis Tao Wan, “Resisting Malicious Packet Dropping in WirelessAd Hoc Networks” Internet draft: draft-ietfitrace-03.txt, January 2003.
[28] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, “Black Hole Attack in MobileAd Hoc Networks” ACMSE’04, April 2-3, 2004, Huntsville, AL, USA.
[29] Muhammad Bohio, Ali Miri, E.cient, “Identity-based security schemes for ad hoc networkrouting protocols” Ad Hoc Networks 2 (2004) 309–317.
[30] SrdjanCapkun and Jean-Pierre Hubaux, “Building Secure Routing out of an Incomplete Setof Security Associations” WiSE’03, September 19, 2003, San Diego, California, USA.
[31] Stallings, W., Wireless Communications and Networks, 2nd Ed., Prentice Hall, 2005.

[32] M. Lamberger, F. Mendel, C. Rechberger, V. Rijmen, M. Schl•aer, Rebound distinguishers: results on the full Whirlpool compression function," Advances in Cryptology, Proceedings Asiacrypt'09, LNCS 5912, M. Matsui, Ed., Springer, Heidelberg, 2009, pp. 126-143.
[33] Bellare, Mihir; Canetti, Ran; Krawczyk, Hugo (1996). "Keying Hash Functions for Message Authentication".
[34] NIST Special Publication 800-38B, “Recommendation for Block Cipher Modes of Operation”: The CMAC Mode for Authentication, May 2005.

Author

Dr Debnath Bhattacharyya received PhD (Tech., CSE) from University of Calcutta, Kolkata, India. Currently, Dr Bhattacharyya associated with Vignan’s Institute of Information Technology, Visakhapatnam-530049, India as Dean R&D of the Institute since the year 2015. His research areas include Image Processing, Pattern Recognition, Bio-Informatics, Computational Biology, Evolutionary Computing and Security. He published 200+ research papers in various reputed International Journals and Conferences. He published six textbooks for Computer Science as well. He is the member of IEEE, ACM, ACM SIGKDD, IAENG, and IACSIT.

