International Journal of Security and Its Applications
Vol. 12, No. 3 (2018), pp.1-10
http://dx.doi.org/10.14257/ijsia.2018.12.3.01

Some Studies on the Security and Space Issues and Challenges in Cloud Computing based Data Centers

N. Thirupathi Rao[1], Ch. Sekhar[1], Debnath Bhattacharyya[1] and Tai-hoon Kim[2*]

[1]*Department of Computer Science & Engineering*
Vignan's Institute of Information Technology (A)
Visakhapatnam, AP, India
[2]*Sungshin Women's University, Bomun-ro 34da-gil,*
Seongbuk-gu, Seoul, Korea
*nakkathiru@gmail.com, debnathb@gmail.com, *taihoonn@daum.net*

Abstract

Dispersed registering has been imagining as the bleeding edge outline of IT undertaking. Disseminated registering shift the submission programming and information places to the gigantic server ranches, where the organization of the data and organizations may not be totally tried and true. With the nearness of the web and the improvement of electronic business entries and relational relations, affiliation done the biosphere marks a generous measure of insights arrange by organize. Additionally, coordinate security issues are at the present time persuading the chance to be essential as civilization is touching towards modernized data age. As a reliably growing number of clients interface with the web it pulls in a broad measure of cutting edge gangsters. It fuses underwriting of access to data in a structure, measured by the scheme chief. This article discussion around the cutting edge for a wide degree of cryptographic considers that are exploited by a bit of systems association submissions. This positions various novel safety confront which contain totally realized. In this paper, we generally spotlight on perspectives for offering safety to information accumulating in dim, furthermore building for information amassing that are realized by additional expert centers dealers in dim, key concentrations for showing safety for further information storing.

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

1. Introduction

A few representations are rupturing up the time of diminish figuring [9], which is a work based change and utilization of PC change. The ceaselessly sensible and all the more viable processors, together with the thing as an affiliation (SaaS) [8] enrolling building, pool relationship on a tremendous level. The widening game plan exchange speed and hard so far adaptable structure affiliations influence it still possible that customers to would now be able to purchase as a top priority blowing relationship from information and programming that harp solely on removed server farm [4]. 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. Along these lines, customers are defenseless before their cloud authority relationship for the openness and reliability of their data. Late downtime of Amazon's S3[4] is such a depiction. Ideal conditions of Cloud accumulating: No persuading inspiration to contribute any capital on restrain

Received (January 15, 2018), Review Result (March 2, 2018), Accepted (March 6, 2018)
* Corresponding Author

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2018 SERSC Australia

gadgets, No need for particular pro to keep up the farthest point, support, replication and essentially calamity association, enabling others to get to your information will happen with communitarian working style rather than specific work.

1.1. Associations in Scattered Enlisting

PaaS [8] pass on figuring resources from side to side a stage. What engineers get with PaaS is a structure they can make to make or re-try demands. PaaS make the development, troublesome, and plan of occupations unbelievable, clear, and financially shrewd, disposing of the need to buy the honest to goodness covering of rigging and programming. One connection between's SaaS versus PaaS needs to do with what points of view must be coordinated by clients, rather than suppliers, totaling, and structures association, however clients compose entries and data. Amazon S3[4] is continue concerning the Internet. It is relied on to impact web-to scale managing less asking for makers. Amazon S3 gives a provoke web affiliations recover any measure of information, at whatever point, from wherever on the web. It gives any fashioner access to the same exceedingly versatile, solid, secure, smart, astute structure that uses its own particular general methodology of targets. The alliance intends to produce purposes behind energy of scale and to pass those ideal conditions on to fashioners. By and by, 4% are utilizing it to hold basic information from their server farms, and a looking at number are utilizing it for close line information securing. In any case, before you take sway and join with an appropriated securing master gathering, there are a few things you have to know. Is appropriated limit secure, What measure of will it cost? What affiliations are best for SMBs. In our left on putting away behind affiliations engineer youngsters, we've collected our best tips and ace asking in one place so you can find answers for your most genuine demand. Find a few game plans concerning cloud post, cloud recording, cloud disaster recuperation, and by methods for the diminish for important common crossroads.

IaaS [8] passes on PC foundation, (for example, a stage virtualization condition), storing, and structures association. As opposed to purchasing programming, servers, or structure hardware, clients can purchase these as a completely outsourced advantage that is everything seen as charged by the measure of central focuses ate up. In a general sense, as a last consequence of a rental cost, an outsider attracts you to show a virtual server on their IT structure. Ascended out of SaaS, PaaS and IaaS clients are responsible for regulating all the more assembling, and structures association. StaaS (Storage as a Service) ordinarily prescribed [5], it inclinations diminish purposes to scale past their obliged servers. StaaS enables clients to hoard their data at remote circles and access them at whatever point from wherever. 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 commitment of neighborhood machines for data fortify in the meantime. Along these lines, customers are defenseless before their cloud expert relationship for the openness and trustworthiness of their data. Late downtime of Amazon's S3 is such an outline. Gushed securing frameworks are relied upon to meet a couple of watchful necessities for keeping up clients' information and data, including high accessibility, intense quality, execution, yet since of the clashing idea of these nuts and bolts, nobody structure sees every last one of them together.

2. Cloud Storage Models

Right now there exists different arrangement of models for dispersed limit that engage clients to keep up oversee in abundance of their data. Circled amassing [2] has framed into three classes, one of which approves the amalgamation of two portrayals for a cost-able and secure choice. Open appropriated amassing suppliers, which show gathering structure as a leasable thing (both regarding entire arrangement and decisively putting away and the systems association transmission restrain utilized inside the foundation).

 Copyright ⓒ 2018 SERSC Australia

Private hazes utilize the contemplations of open dispersed accumulating yet in a packaging that can be safely presented inside a client's firewall. Ultimately, cross breed spread limit empowers the two models to unite, engaging blueprints to depict which information must be kept up stealthily and which can be secured inside open hazes.

The diminish copy is indicated graphically in the above Figure 1. Cases of open circled storing providers unite Amazon (which offers amassing as an association). Occasions of private appropriated storing providers join IBM[1], Para scale, and Clever safe (which influence programming and furthermore to intend for inward mists). At last, cross breed cloud providers meld Egnyte, among others. While these electronic online affiliations do give goliath measures of storage space and versatile selecting resources, this figuring stage move, regardless, is shedding the devotion of neighborhood machines for data fortify meanwhile. Along these lines, customers are defenseless before their cloud master relationship for the availability and trustworthiness of their data. Late downtime of Amazon's S3[4] is such a depiction.

Data storage room wellbeing structures in flowed figuring an assortment of realistic strategies [2] have been broke down in this paper. Spread accumulating is viewed as a strategy of scattered server develops that everything considered make utilization of virtualization advancement and arrangements fringe for data putting away. Incontestable storage room wellbeing to data in online insofar as fathomed restrict security to data in online is more profitable in a passed on preparing. The utilization of an information isolating arrangement for finishing such security including the foundations of a polynomial in compelled field. In this course of action information is distributed such way that each piece is clearly sheltered and don't to be prearranged. These bits are secured on various servers on the system which are known just to the client. Entertainment of the information suspects that passages will every server and the learning as to which servers the information allotments are secured. A few kinds of this game plan are delineated, which join the obvious putting away of encryption.

Perceive: A see based encryption (IBE) and translating and character based stamp IBS prepares. Assets and associations are passed on completed diverse client. So there is a measurements of different security dangers. Thusly check of clients and moreover associations is an irreplaceable fundamental for obscure wellbeing. Precisely when SSH Authentication convention (SAP) was utilized to cloud, it winds up being astoundingly mind boggling. As another contrasting option to SAP, proposed another endorsement custom in context of character which depends upon various leveled show with relating engraving and encryption framework. See based endorsement custom compels social occasion of steps.

Validity at scheming servers is the bona fide worry in spread limit with open review confine trusted segment with limit and points of confinement information proprietors don't packs can be doled out as an outer review party to get to the danger of outsourced information when required. It besides gives a direct yet sharp strategy for information proprietors to get confidence in the diminish. To achieve, dynamic information strengthen, the existent change of PDF (or) POR conspire is enhanced by defaming the fundamental Markel Hash tree (MHT). Cloud clients set away data in obscure server with the target that wellbeing and in addition data aggregating precision is essential concern. The data proprietors having tremendous measure of outsourced data and examining the data rightness in a diminish situation can be troublesome and costly for information proprietors. To help pariah surveying where client securely name in respectability checking assignments to untouchable auditors(TPA)[2] this course of action have the capacity to roughly confirmation the simultaneous requirement of data mistake(*i.e.*, the ID of creating an uproar servers). A story and uniform plan knows about offer wellbeing to different obscure makes. To achieve data gathering security, BLS (Bonch-Lynn-Sachems) tally is adjusted with meaning the information disappoints past to outsourcing data into

Copyright ⓒ 2018 SERSC Australia

diminish. Reed Solomon strategy is use for bungle correction and to ensure information hoarding change.

Method for amassing is diminish won't not be totally great to put stock in perspective of the light of the data that the customers don't have neighborhood duplicate of informational collection gone in diminish. To manage these issues made arrangements for one more convention structure utilizing the information looking at custom estimation to check the information respectability associations be achievable altered information investigating calculation. The data proprietors having huge measure of outsourced data and breaking down the data rightness in a diminish situation can be troublesome and costly for information proprietors. An adaptable scattered amassing reliability investigating fragment (FDSIAM), these systems decimation and not blocking issues and passed on cancelation angled data.

Persuading and safe storage room methodology is the present case for clients which subcontract information into master affiliation the individuals who having an adequate area for restrain with chop down cutoff cost. An ensured and fruitful putting away custom is arranged that confirmation the data amassing secret and dependability. The present convention is imagined by methods for the headway of elliptic curve cryptography and calm social event is utilized to demand the data honesty[2]. Data and programming technique convention pace executed by obscure customers to put in the affirmation essential structure to the thing and information before exchanging them to the cloud. Test reaction custom is convention is attestation with the target that it won't uncover the substance of the information to untouchables. Data vivacious process is in like way utilized keep a practically identical security affirmation what's more offer facilitating to clients from the troublesome of information spillage and degradations issues.

2.1. Limit Security of Data

The information is tenable in server in perspective of customer's choice of security strategy with the objective that information is known eminent protected need possessions are being common transversely finished server burden to information security in blur. Broadcasting information above web is hazardous as a result of the interloper attacks data encryption expects a basic part in cloud condition. Displayed a solid and novel structure for offering security to cloud makes and completed an ensured cross stage. A protected and successful storing tradition is planned that assurance the information accumulating mystery and trustworthiness. The current tradition is envisioned by means of the advancement of elliptic twist cryptography and quiet gathering is employed to insist the information honesty. The proposed convincing and versatile dispersal plot two-route handshakes in light of token organization by make use of the homomorpic voucher with circled affirmation of cancellation coded data, our arrangement attains the coordination of limit precision assurance and data botch territory (*i.e.*,) the conspicuous verification of misbehaving server.

3. Safety and Security Issues of Cloud Storage Space

Storage organization of stipends customers to the information in blurs and furthermore allowable to make use of the open especially capable request with no pressure data accumulating kept up. Despite the way that cloud providers' benefits, such an organization surrenders the balance of customer's data that familiar new valuability hazards with cloud data rightness. The proposed a versatile spread amassing dependability assessing instrument, employ the homomorphism voucher and coursed coded-data. The information proprietors having gigantic 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 safe and successful lively process on subcontract information counting piece alteration, removal and join.

 Copyright ⓒ 2018 SERSC Australia

Perfect conveyed stockpiling structures dim information accumulating which need no attempt is getting more noteworthy commonness for human being, enterprise and foundations information support and synchronization. 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 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[4] is such a delineation. A protected and successful storing tradition is planned that assurance the information accumulating mystery and trustworthiness. The current tradition is envisioned by means of the advancement of elliptic twist cryptography and quiet gathering is employed to insist the information honesty. The proposed structure depicts, at an irregular express, a possible designing for a cryptographic accumulating organization.

Strategy of access and store little records with ability to help benefits extensively, Hadoop scattered archive structure server reasons are investigated for little record bother of neighborhood Hadoop appropriated report system. Weight on Nane Node of HADOOP flowed record structure is maintained by tremendous measure of little archives, for data course of action amendment are not considered perfecting part isn't 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 particularly joined limit and execute customer application undertaking.

Record accumulating security organization to ensure the security of set away data in cloud, presented a structure which utilizes flowed plot. Proposed structure contains a pro server and a course of action of slave server. These are not quick substitution associate among customers and slave servers in the projected show. Expert server is able to procedure the customer’s demand and at slave server piecing process to give data fortification to record revival in outlook. Clients archive is secured as tokens on principal server and records were pieced on slave server for report recovery. The information proprietors having gigantic measure of outsourced information and analyzing the information rightness in a dim circumstance can be troublesome and expensive for data proprietors. A protected and successful storing tradition is planned that assurance the information accumulating mystery and trustworthiness. The current tradition is envisioned by means of the advancement of elliptic twist cryptography and quiet gathering is employed to insist the information honesty.

The most for the part observed of these sorts are paying little mind to the way which rely on the old convention. All these APIs are related with working up requests for advantage by procedures for the Internet. REST is a thought everything considered clears as an approach to manage 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 isn't required. It is fundamental in light of how the Internet is out and out inert (it has a conflicting response time and it is all things considered not snappy when risen up out of a zone is an approach that has high proclivity to the way the Internet works. Standard annal hoarding access techniques that utilization NFS (arrange records structure) or CIFS (Common Internet File System)[7] 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. Thusly, customers are

Copyright ⓒ 2018 SERSC Australia

defenseless before their cloud pro relationship for the availability and reliability of their data. Late downtime of Amazon's S3[4] 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 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 way the snappiest making information all together.

It gathers that the essential and particular confirmation is by an application. APIs are vernacular sensible and in this way can be make utilization of productively by engineers abuse any advance tongue they pick. Belonging inside the structure quality are going at the go down on from side to side a URL. Along these lines, an API isn't a "programming vernacular", yet tongue is make utilization of to get beyond what many would consider possible cloud. REST APIs are correspondingly about changing the state of favored outlook from side to side outlines of those focal points. They are not tied in with livelihood work advantage frameworks in an achievable sense. The enter complexities flanked by interesting dark storage space APIs are the URLs depicting the points of interest and the strategy of the outlines.

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 distant 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 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[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. The most generally perceived sorts of remote security. 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 acknowledge 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 principle limitations of remote Web get to: the obstructions of the compact center (little screen assess, confined data capacity) and the low data rates of remote automated frameworks. Two basic WTLS thoughts are the ensured session and the sheltered affiliation, which are portrayed in the specific as: 1) Secure affiliation: An affiliation is a vehicle (in the OSI layering model definition) that gives a fitting sort of organization. For SSL, such affiliations are shared associations. The affiliations are transient. Every affiliation is connected with one session. Between any join of social events (applications, for instance, HTTP on client and server), there may be different secure affiliations. On a basic level, there may in like manner be distinctive synchronous sessions between parties, however this segment isn't used as a piece of preparing.

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

 Copyright ⓒ 2018 SERSC Australia

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 distant 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 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[4] is such a delineation. The term is much of the time associated with scrambling plaintext message into ciphertext by then back yet again (known as interpreting).

5.1. Riddle Key Cryptography

All things considered, the same plaintext square will reliably encode to the same ciphertext while using a comparable key in a piece figure while the same plaintext will scramble to different ciphertext 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 mode is the minimum unpredictable, most clear application: the secret key is used to scramble the plaintext square to shape a ciphertext piece. Two indistinct plaintext squares, by then, will constantly deliver the same ciphertext piece. Disregarding the way this is the most common Secret key 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 ciphertext in a stream figure. Square figures can work in one of a couple of modes; the going with four are 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 indistinct military term of a fight confining geographical component). Firewalls can make choke centers 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, firewall can be used to complete VPNs. Firewalls can in like manner bind sort out presentation by covering the internal framework structure and information from individuals as a rule Internet. A firewall may be expected to fill in as a channel at the level of IP packages, or may work at a higher tradition layer. IaaS[8] passes on PC establishment, (for instance, a phase virtualization condition), hoarding, and structures affiliation. Rather than buying programming, servers, or structure equipment, customers can buy these as a totally outsourced advantage that is everything viewed as charged by the measure of focal points ate up. In a general sense, as a last result of a rental cost, a pariah draws in you to display a virtual server on their IT structure. Risen up out of SaaS, PaaS and IaaS customers are accountable for administering more gathering, and structures affiliation.

Copyright ⓒ 2018 SERSC Australia

6.1. Kinds of Firewalls

A firewall may go about as a bundle channel. It can fill in as a positive channel, allowing passing just packages that meet specific criteria, or as a negative channel, expelling any package that meets certain criteria. StaaS (Storage as a Service) usually recommended [5], it urges dim purposes to scale past their obliged servers. StaaS empowers customers to amass their information at remote circles and access them at whatever point from wherever. 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 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 S3is such a delineation. Streamed putting away systems are depended on to meet a few vigilant necessities for keeping up customers' data and information, including high availability, fervent quality, execution, yet since of the conflicting thought of these basics, no one structure sees each and every one of them together.

Dependent upon the kind of firewall, it may examine no less than one tradition headers in each package, the payload of each package, or the illustration delivered by a game plan of groups. Sorts of firewalls are showed up in Figure 8.

6.2. Package Filter

A package channel is a unique firewall that techniques organize development on a package by-package introduce. 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 can't turn away ambushes that use application-specific vulnerabilities or limits. For example, a package channel firewall can't square specific application charges; if a package channel firewall allows a given application, all limits available inside that application will be permitted. Package channel firewalls are all things considered defenseless against strikes and tries that adventure issues inside the TCP/IP detail and tradition stack, for instance, organize layer address spoofing. Various package channel firewalls can't 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.

6.3. Stateful Packet Inspection

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 analyze confined measures of usage data for some remarkable traditions like FTP, IM and SIPS charges, remembering the true objective to recognize and track related affiliations.

7. Conclusion

Information storing in 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 an unpreventable stress for any affiliation whose inward private framework is related with the Internet. The security for the data has ended up being significantly key. Customer's data security is a central request over cloud. This paper rapidly displays the possibility of

 Copyright ⓒ 2018 SERSC Australia

PC security, bases on the perils of PC compose security later on and work ought to be conceivable on key scattering and organization and furthermore perfect cryptography estimation for data security over fogs. The authors mainly based on data amassing points that cloud master associations are pursue 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 (TPA)[2] frameworks which are used for information build up and safety for information in dim. The analysis we had discussed and the results we had discussed with the comparison from the previous set of results and previous results will give us a good idea about the working and performance style of the current considered model.

References

[1] S. Nandan Kumar, "Technique for Security of Multimedia using Neural Network", Paper id-IJRETM-2014-02-05-020, IJRETM, vol. 02, no. 05, **(2014)** September, pp. 1-7.
[2] A. Simmonds, P. Sandilands and L. van Ekert, "Ontology for Network Security Attacks", Lecture Notes in Computer Science. Lecture Notes in Computer Science, 3285, **(2004)**, pp. 317-323.
[3] M. Bellare and P. Rogaway, "Introduction", Introduction to Modern Cryptography, **(2005)** September 21, pp. 10.
[4] A. J. Menezes, P. C. van Oorschot and S. Vanstone, "A Handbook of Applied Cryptography", ISBN 0-8493-8523-7.
[5] R. Davis, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, vol. 16, no. 6, **(1978)** November, pp. 5-6.
[6] S. NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, **(2004)** May.
[7] J. Daemen and V. Rijmen, "Rijndael: AES-The Advanced Encryption Standard", Springer, Heidelberg, **(2001)** March.
[8] FIPS 197, Advanced Encryption Standard, Federal Information Processing Standard, NIST, U.S. Dept. of Commerce, **(2001)** November 26.
[9] B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings (Springer-Verlag), **(1993)**, pp. 191-204.
[10] B. Schneier, (2005-11-23), "Twofish Cryptanalysis Rumors", Schneier on Security blog. Retrieved 2013-01-14.
[11] M. Matsui and T. Tokita, "MISTY, KASUMI and Camellia Cipher Algorithm Development", Mitsibishi Electric Advance (Mitsibishi Electric corp.), ISSN 1345-3041, vol. 100, pp. 2-8.
[12] General Report on the Design, "Speification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms", 3GPP, **(2009)**.
[13] O. Dunkelman, N. Keller and 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)**.
[14] R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communication of the ACM, vol. 21, no. 2, **(1978)** February.
[15] W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, vol. 22, no. 6, **(1976)**, pp. 644-654.
[16] N. Koblitz, "Elliptic curve cryptosystems", Mathematics of Computation, vol. 48, **(1987)**, pp. 203-209.
[17] V. Miller, "Use of elliptic curves in cryptography", CRYPTO 85, **(1985)**.
[18] FIPS 180, "Secure Hash Standard", Federal Information Processing Standard (FIPS), Publication 180, NIST, U.S. Dept. of Commerce, **(1993)** May 11.
[19] M. Lamberger, F. Mendel, C. Rechberger, V. Rijmen and M. Schlaer, "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.
[20] M. Bellare, R. Canetti and H. Krawczyk, "Keying Hash Functions for Message Authentication", **(1996)**.
[21] NIST Special Publication 800-38B, "Recommendation for Block Cipher Modes of Operation", The CMAC Mode for Authentication, **(2005)** May.

Copyright ⓒ 2018 SERSC Australia

Authors

Dr. N. Thirupathi Rao received Ph.D. from Andhra University, Visakhapatnam, India. Currently, Dr. Rao is associated with Vignan's Institute of Information Technology, Visakhapatnam-530049, India as Assistant Head of Computer Science and Engineering. His research areas include Communication Networks, Mathematical Modeling, Image Processing, Pattern recognition, Evolutionary Computing and Security. He published 55+ research papers in various reputed International Journals and Conferences. He is the member of IE Kolkata, ACM, ISPS, CSI.

Dr. Debnath Bhattacharyya received Ph.D. (Tech., CSE) from University of Calcutta, Kolkata, India. Currently, Dr. Bhattacharyya is associated with Vignan's Institute of Information Technology, Visakhapatnam-530049, India as Head of Computer Science and Engineering and 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 6 text books for Computer Science as well. He is the member of IEEE, ACM, ACM SIGKDD, IAENG, and IACSIT.

Dr. Tai-hoon Kim received B.E., and M.E., degrees from Sungkyunkwan University in Korea and Ph.D. degrees from University of Bristol in UK and University of Tasmania in Australia. Now he is working for Department of Convergence Security, Sungshin W. University, Korea. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments. He published 400+ research papers in various reputed International Journals and Conferences. He published 10 text books for Computer Science as well. He is the member of IEEE, ACM, etc.

 Copyright ⓒ 2018 SERSC Australia