DOI:10.22413/ijastems/2020/v7/i2/1

ARSM hybrid hash algorithm based optimal solution approach and implementation for improved cloud security defensive mechanism

Srinivasa Rao G [1] ,Panem Charan Arur [2] ,Manjunath Ramanna Lamani[3]

Ph.D. Research Scholar, Dept of Computer Science , Dravidian University, Andhra Pradesh, India [1]

Faculty, Department of ECE, GEC, Karwar,Karnataka[2]

Faculty, Department of CSE, GEC, Karwar,Karnataka[3]

Abstract— Cloud is a technically updating, sophisticated interactive, distributed phenomenal, computational technological environment, with its collection of heterogeneous services under a single umbrella. With the help of cloud it is possible to create any service, is possible to adjust its configuration, they can be customized and they can store their data online. Cloud technology has two main problems. First one is challenges from cloud itself in its maintenance like proper scheduling, balancing the load. Optimal computing resources utilization could solve the problem. The second one is cloud resources are virtualized. Virtualization of resources has not only brought technological advancement but also brought some new challenges which are prone to get serious threats to the integrity of the data and its security. There are many sorts of security mechanisms to secure the data. Cryptography is one of them. Cryptography is a science of intelligence and an art of secrecy. The existing mechanisms have their own limitations. A literature glance view is provided to illustrate the possible attack mechanisms in cloud computing environment and the existing solutions. ARSM Hybrid hash algorithm is proposed for the security defensive mechanism and its research methodology is provided. ARSM is a Hybrid hash algorithm with a combination of SHA-256, AES, RSA and MD5 algorithms. The limitations of these individual algorithms have driven to combine them. As per the analysis it is found effective over the considered other techniques. Present study is aimed to find an optimal solution for Threat detection, prevention and effective defence mechanisms for the security in Cloud using any hybrid hash algorithm and to implement.

Index Terms— Cloud Computing, Security, Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), Hybrid Algorithm, Hash functions, Secure Hash Algorithm (SHA256), Encryption, Decryption, Cryptography, Security, Confidentiality, Integrity, Authorization.

I. INTRODUCTION

Cloud is a technically updating sophisticated computing environment. It is a distributed environment in which ‘computing resources are shared across the users simultaneously’. Meaning of ‘computing’ is now upgraded from a ‘simple desktop computing application’ to the ‘distribution computing application’. This pay and use model has provided Softwares, Platforms and Infrastructures as services to the end-user on demand. One does not need to buy servers and worry about their storage along with the services and applications. Therefore it is an ‘on demand network oriented resource pooling mechanism’ for the reduction of capital cost on hardware and software [1].

Cloud is a ‘specialized environment’ with a huge collection of computer systems which are connected to internet with either public network (or) private networks. This cloud environment provides facility to the end user on demand. Cloud computing is a ‘collection of heterogeneous services under a single umbrella of cloud service provider’. Therefore in many cases the end-user need not for the installation or acquire new devices to having any specialized services. An example for this is Google provides many of its services like Gmail, Google docs, Google maps etc which does not demand any installation and need to connect any new devices. Similarly Microsoft is providing its cloud services Microsoft Office 365 and Microsoft azure. Sales force and Amazon are also providing their services to their consumers as per the needs [2].

II. AIM OF THE STUDY

Aim of study is to find an optimal solution for Threat detection, prevention and effective defense mechanisms for the security in cloud using any hybrid hash algorithm and to implement.

III. ORGANIZATION OF THE PAPER

The organization of the paper is as follows:

Title of the Paper

Abstract

Key words

1. Introduction

DOI:10.22413/ijastems/2020/v7/i2/1

2. Aim of the study
3. Organization of the paper
4. Cloud computing and it's technical back ground
5. Scheduling - load balancing - optimal computing resource utilization
6. Resources virtualization
7. New technologies and security challenges to the cloud resources in new era
8. A glance view on types of possible attack mechanisms in cloud and existing solutions - a literature review
9. Proposal of ARSM hybrid hash algorithm for the security defensive mechanism - research methodology - a Discussion
10. Analysis
11. Results obtained
12. Advantages of proposed methodology
13. Limitations of present study
14. Conclusions
15. Scope for the future work

Acknowledgment
Funding Statement
Conflict of Interest
References

IV. CLOUD COMPUTING AND IT'S TECHNICAL BACK GROUND

The father of cloud computing John Mc Karthy has a wish to have computing 'as- a- utility' and he aspired for the massive participation of the general public. His motto has been accomplished with cloud computing [3].

'Resource usage can be monitored, controlled, and reported by the provider and end-user' in cloud computing environment. Working models may differ by any other means, but it is intended for the efficient utilization of computational resources along with reaching the end-user. Cloud is an 'interactive technology' that provides the resources as per the needs of the user [4].

Virtualization helps to slice the data center to act like many numbers of servers. Even though it depends on the hardware configuration, there is a need for software to analyze and give a calculation of how many virtual machines are needed and how they can be divided to implement virtualization. Such softwares are commercially available today to improve performance for example Microsoft Azure [5].

V. SCHEDULING - LOAD BALANCING - OPTIMAL COMPUTING RESOURCE UTILIZATION

Cloud computing is a collection of heterogeneous environments; thereby the nature of the user-requests also reflects the same. User requests need different computational requirements, and they vary from time to time. Peak hours and non-peak hours makes a good factor in predicting the resource requirements [6]. During the peak, hours more resources need to be made available to handle the situation.

'Response time' is a time in which a job or an activity becomes activated. Response time would be longer than the execution time in an operating system [7].

CPU is one of the most critical parts of the computer. Multiprogramming is one of the basic and important scheduling techniques. Generally, CPU scheduling is done in such a way as to keep it busy as much as possible [8].

Scheduling occurs due to any one of the four conditions such as the given below (i) When a process has gone from switching state to waiting for state or (ii) When a process is terminated or (iii) When a process switches from running state to the ready state or When a process switches from waiting for the state to the ready state [9].

Scheduling performance can be evaluated using a synthetic workload below the parameters (i).Distribution of several tasks, (ii). Distribution of real-time job services on demand, (iii).Average inter-arrival time of tasks, (iv).Period of real-time jobs. Scheduling policies can be stated as below (i).FCFS (First Come First Serve), (ii).Round Robin (Execution of tasks in a cyclic manner), (iii). Shortest Job First (SJF) etc are a few to name [10].

Generally, the cloud user needs the tasks to be completed with below average makespan (completion time of the given job), with below average computational cost, below average turnaround time, and with below average response time. At the same time, the cloud provider needs below average resource utilization, more throughputs, energy efficiency, and a balanced load [11].

Cloud computing is generally considered as on-demand service [12].

As soon as the load is allotted to the node it cannot be transferred to another node. This approach requires below average communication, as a result, reduces the execution time [13].

Some of the issues like Electricity consumption depend on the size and the number of servers used. Data Center usually consumes 0.1 MW to 15 MW. Power Usage Effectiveness (PUE) is used to estimate the power usage in Data Centers [14].

Even though Moore's Law says about the increment of performance of transistors every approximately 730days, in case of power consumption there is no much improvement is evident.

DOI:10.22413/ijastems/2020/v7/i2/1

VI. RESOURCES VIRTUALIZATION

Server virtualization can be used for different virtual machines with different operating systems on the same physical system. It is virtualization which is both one too many and many to one concept [16].

Computing tasks are distributed in cloud computing. These tasks are mapped to a pool of resources. In a single computer system, it can create many numbers of virtual machines. If any host needs, it could be easily transferred its working load to another host with below average interruption [17].

Live virtual machine migration can be achieved in any one of two types [18].

They are, (a).A control mechanism is switched to the destination. (b).Data is transferred to the destination: this data transfer can be achieved in any one of the following: (i). Pre copy: This type of copy allows transferring the memory to the destination first and the execution is transferred later. (ii). Post copy: This type of copy allows us to transfer the execution to the destination first and then the memory later.

VII. NEW TECHNOLOGIES AND SECURITY CHALLENGES TO THE CLOUD RESOURCES IN NEW ERA

Multi-Cloud Exchanges to Optimize Connectivity Today, multi-cloud exchanges offer the next level indirect connectivity, allowing organizations to safely and easily expand multi-cloud capabilities. Exchanges eliminate the added worries that an open Internet can bring as well as the tedious provisioning and configuring that comes with connecting to the public Internet [19].

Now- a- days security to the data in the cloud computing is highly at risk. It is not possible to view data at risk separate from cloud computing environment. Therefore security provisioning is must for the data in cloud environment. It is not easy to provide such desired security on demand [20].

VIII. A GLANCE VIEW ON TYPES OF POSSIBLE ATTACK MECHANISMS IN CLOUD AND EXISTING SOLUTIONS - A LITERATURE REVIEW

Here are a few terms often used in this crypto science such as, Alice is the Sender of the message, Bob is the Receiver, Eve is an Eavesdropper or unintended party, Plaintext is a Message to be sent, Ciphertext is a Coded message, Encryption is a Coding of message, Decryption is a Decoding the message, Cryptology is a Science of study of ciphers, Cryptography is a Science of encrypted communication between Alice and Bob, such that even if Eve intercepts the ciphertext, she won't be able to make any sense of it [21].

There are some cryptanalysis tools available. They are,

(i). CrypTool: CrypTool aims at making people understand network security threats and working of cryptology. It includes asymmetric ciphers like RSA, elliptic curve cryptography.

(ii). CT2 has an improved GUI and more than hundred cryptological functions.

As per Dr. Balachandra, The Cloud computing related security mechanisms and the data integrity is possible to manage provided when proper scheduling mechanisms are taken. Authenticity is the features which need to focus [22].

As per Alshammari Hamoud, Managing the performance of Security and its related issues are possible to control using very strong service level agreement and the authenticated login processes could reduce the risk of un-wanted intruder.

Manavi Sina has proposed a model to security based mechanism for the detection of un-wanted intrusion by the hacker. It uses a detection mechanism by the combination of virtualization concept with the attacker alarming mechanism. As per Shina Sheen, there are mainly three varieties of ways to make the cloud away from easy intrusion. It is a filter based method. A decision tree based algorithm would help to do so. As since the electronic age transforming into sophistication, the intruder (or) peepers getting up advanced. The more technology is advanced the hackers maximizing their technological ability to reduce the confidence of the end-user [23].

Vanishreeprasad. S and Mrs. K N Pushpalatha (2015) have improved the data security by proposing an architecture that integrates the cryptographic algorithms, Advanced Encryption Standard (AES) algorithm and the Hash function, SHA-2.

Bernd Gastermanna, Markus Stopper, Anja Kossik, and Branko Katalinic (2015) have proposed and implemented a secure cloud storage solution for small and medium-sized enterprises (SMEs) [24].

IX. PROPOSAL OF ARSM HYBRID HASH ALGORITHM FOR THE SECURITY DEFENSIVE MECHANISM - RESEARCH METHODOLOGY – A DISCUSSION

Research Questions Part

Q-1: What is the aim of the present study?

Q-2: What is the technical background of the cloud computing?

Q-3: What is the role of cloud resources in the maintenance of cloud?

Q-4: What is scheduling, load balancing, and optimal computing resources utilization?

Q-5: What is resources virtualization?

DOI:10.22413/ijastems/2020/v7/i2/1

Q-6: What are new technologies and what are the security challenges to the cloud resource in the new era?

Q-7: As a glance view what are the types of possible attack mechanics in cloud and what the existing solutions available now?

Q-8: What are the cryptographic algorithms are available and their pseudo codes?

Q-9: Is it possible to find new solutions to the existing problems?

Q-10: Whether if any proposed methodology are the advantages over the existing mechanisms?

Q-11: What are the limitations of such proposed methodology?

Q-12: Is there any future scope for such work for the extension?

Cryptography and a Glance view

Modern crypto systems depends one key. The keys are two types. The first one is 'Public Key' which is a key which is known to all. The name itself suggests that 'Publicly Known Key'. The second one is 'Private Key' which is un-like the public key, it is known only to the owner of the key [24].

SHA-256 Hash Function

SHA-256 is a hash function based cryptographic mechanism. It is a secured Hash algorithmic method. Hash is a digital data math operation. Only by processing the hash it is possible to get the integrity of the data. In this mechanism data is make two parts like 64 bits each. It is issued with some 256 bit based hash code [25].

SHA-256 is a Hash function for the security for the data. Generally the hashes are like the signature for a complete set of information stored in digital format. The word SHA-256 means 256 bit oriented message digest. The Message digest is a function which works in one way. It is not easy to tamper. It is a more secured and it is generally used in Digital Signatures.

Disadvantages of SHA-256: The advancements in hardware have made it decrypt this hash message with some stringent efforts.

Therefore one needs to find some improvements in this regard [26].

AES Encryption

AES (Advanced Encryption Standard) algorithm is a symmetric key based algorithm. In this algorithm there would be a common key for the encryption and decryption both [27].

Disadvantage: This is prone to Brute force algorithm based attacks and side channel attacks.

Therefore one needs to find some improvements in this regard.

RSA based key generation

RSA (Rivest-Shamir-Adleman) algorithm is an asymmetric key based algorithm. In this algorithm there would be two keys for the encryption and decryption [30].

Disadvantage: MD5 is having problem from hash collision weakness. Due to this problem the hacker is able to get a chance to make several number of and variety of inputs as of when this technique is utilized, by providing the same result [31]

ARSM Hybrid hash algorithm

The combination of AES, RSA, SHA- 256, MD5 can be called as ARSM Hybrid Algorithm. This mechanism encrypts the given data using the combination of algorithms. It is a layered mechanism of encryption and decryption routines for multiple numbers of times. This process is repeated for a next round of 64 times. It has the maximum message size capacity of 33 bytes and 4 bytes word size is possible. This mechanism runs with 140 MiB/s of speed.

(i). Working Mechanism Approach for UPLOAD Process

Step -1: The end-user uploads his/her file from a remote system

Step -2: The system would generate a key. The key is for the process of encryption mechanism

Step -3: The complete file is encrypted using the key.

Step -4: The system would generate a secret hash key.

Step -5: The file which is encrypted is send to the data base server.

Step -6: The information in the file along with the hash key would be secretly stored inside the database server.

(ii). Proposed Working Mechanism Approach for DOWNLOAD Process

Step -1: Verification process for the file.

Step -2: System decryption mechanism for the file.

Step -3: File download and delivered to the end-user.

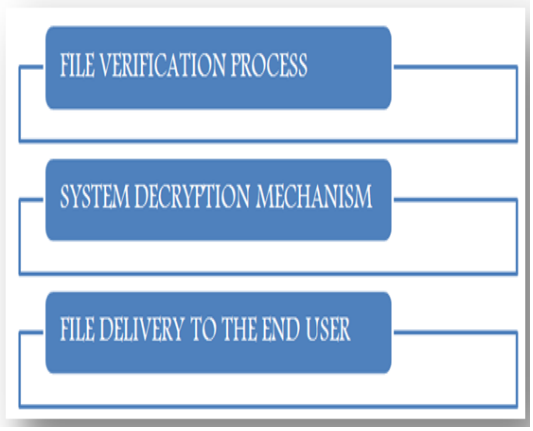


Fig.3. Download process for the proposed methodology

DOI:10.22413/ijastems/2020/v7/i2/1

TEST Environment (TEST BED)
System Requirement
Hardware Requirement
Processor - Dual Core
Speed - 1.1 G Hz
RAM - 512 MB (min)
Hard - 20 GB
Key Board - Standard Windows Keyboard
Mouse - Two or Three Button Mouse
Hardware Requirement
Operating System : Windows xp,7,8
Front End : Java 7
Technology : Swings,Core java
IDE:Netbeans.

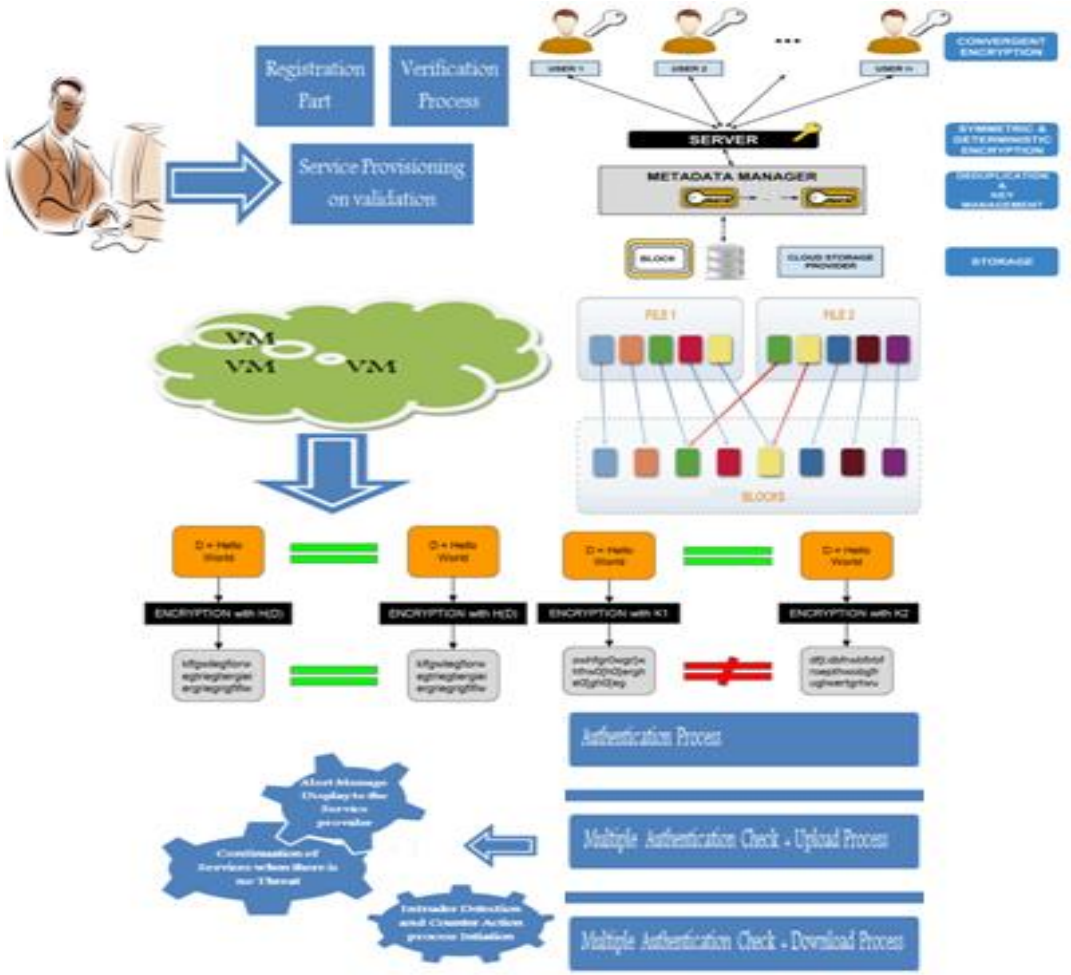


Fig.4. ARSM Hybrid hash algorithm Working Mechanism Architecture Diagram

X. ANALYSIS

The end-user needs his/her data need to be stored processed and transmitted safely and securely. At the same time the cloud service provider would try to find for optimization techniques that would allow them to do so. It can be done using with this issue by adding one additional layer of deterministic and symmetric encryption on top of convergent encryption. This additional encryption can be added by a component placed between the user and the cloud service provider such as a local server or a gateway.

DOI:10.22413/ijastems/2020/v7/i2/1

This component will take care of encrypting/decrypting data from/to users. In order to allow the cloud provider to detect duplicates, encryption and decryption are performed with one unique set of secret keys. This set of secret keys is securely stored by the component and won't be shared with anyone for any reason. As we can see, one simple additional layer of encryption is sufficient to keep de duplication feasible and prevent the cloud provider from performing any of the above-mentioned attacks. Indeed, the cloud provider will never access these secret keys. This simplest solution would be to make users store their keys, but this would be unpractical since it would require a considerable amount of storage space.

The complete system structure would like as given below:

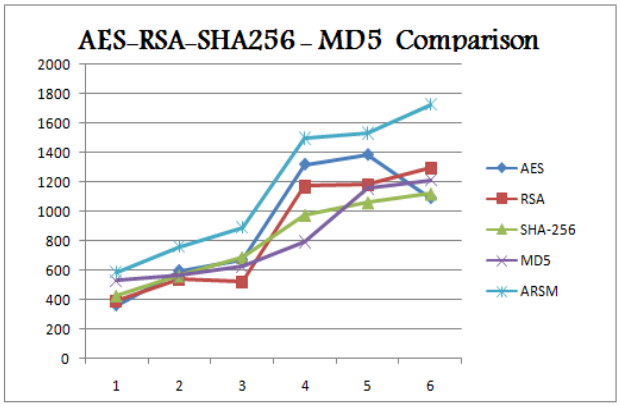
We have a number of users who, before uploading to the Cloud, split data into blocks, encrypt blocks with convergent encryption and send to the server encrypted blocks together with their associated encrypted keys. A server that further encrypts blocks and keys with a set of unique and secret keys. A metadata manager that updates the metadata in order to rebuild the structure of each file, stores encrypted block keys and performs de duplication on encrypted blocks. Only those blocks that are not already stored are actually stored. A storage layer to store single blocks, which can be seen as files of lesser size. Since our system is completely storage agnostic, we can implement the storage layer with any storage system. For instance, we might use a cloud storage provider such as Amazon S3, a distributed storage, a local file system, etc.

XI. RESULTS OBTAINED

AES, RSA, SHA-256 and MD5 algorithms are considered for the testing with different inputs. The proposed Algorithm ARSM is also tested in this environment. However the respective algorithms are supplied with the inputs of 25kb, 35kb, 55kb, 65kb, 85kb and 95kb. The results are obtained. They are provided in the given below Table-1.

Input Data Size in Kb	Execution Time in milliseconds				
	AES Algorithm	RSA Algorithm	SHA-256 Algorithm	MD5 Algorithm	ARSM Algorithm (Proposed)
25	362	389	427	529	587
35	597	535	563	564	762
55	673	521	689	623	893
65	1321	1169	978	793	1498
85	1387	1183	1063	1158	1533
95	1093	1294	1122	1213	1728

Table-1. Comparison performances of encryption execution time all algorithms at a time.



Graph-1. Comparison performances of encryption execution time all algorithms at a time.

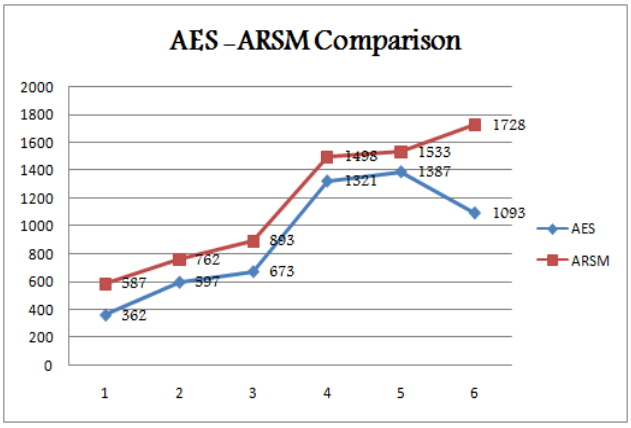
XII. ADVANTAGES OF PROPOSED METHODOLOGY

(Observed Improvements in proposed methodology)

AES, ARSM algorithms are considered for individual comparison. The results are tabulated as given below in Table-2.

Input Data Size in Kb	Execution Time in milliseconds		
	AES Algorithm	ARSM Algorithm (Proposed)	Difference in milliseconds
25	362	587	225
35	597	762	165
55	673	893	220
65	1321	1498	177
85	1387	1533	146
95	1093	1728	635

Table-2. Comparison performance of encryption execution time AES and ARSM.



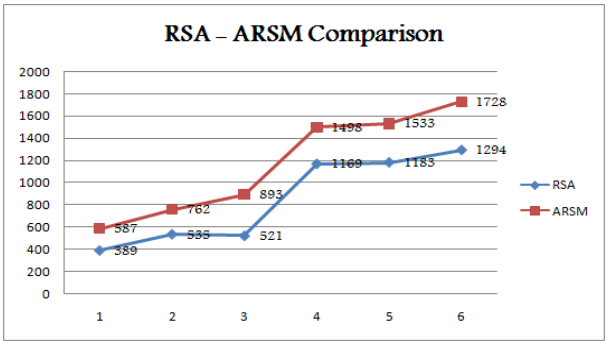
Graph-2: Comparison performance of encryption execution time AES and ARSM.

AES, ARSM algorithms are considered for individual comparison. The results are tabulated as given below in Table-3

DOI:10.22413/ijastems/2020/v7/i2/1

Input Data Size in Kb	Execution Time in milliseconds		
	RSA Algorithm	ARSM Algorithm (Proposed)	Difference in milliseconds
25	389	587	198
35	535	762	227
55	521	893	372
65	1169	1498	329
85	1183	1533	350
95	1294	1728	434

Table-3. Comparison performance of encryption execution time RSA and ARSM.

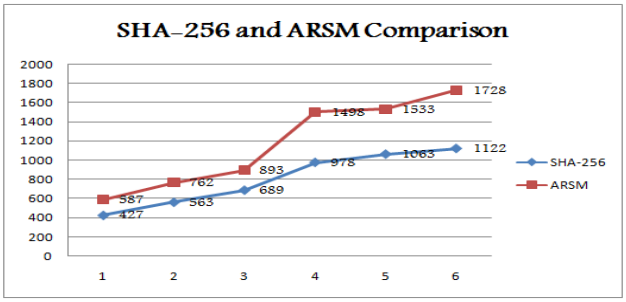


Graph-3: Comparison performance of encryption execution time RSA and ARSM.

SHA-256, ARSM algorithms are considered for individual comparison. The results are tabulated as given below in Table-4.

Input Data Size in Kb	Execution Time in milliseconds		
	SHA-256 Algorithm	ARSM Algorithm (Proposed)	Difference in milliseconds
25	427	587	160
35	563	762	199
55	689	893	204
65	978	1498	520
85	1063	1533	470
95	1122	1728	606

Table-4. Comparison performance of encryption execution time SHA-256 and ARSM.

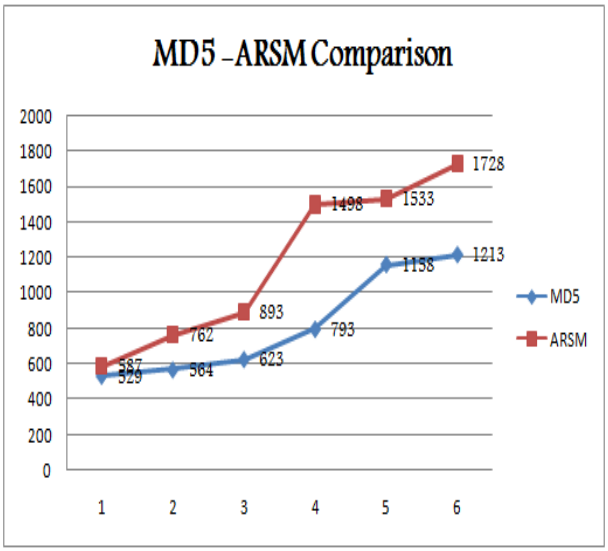


Graph-4: Comparison performance of encryption execution time AES and ARSM.

MD5, ARSM algorithms are considered for individual comparison. The results are tabulated as given below in Table-5.

Input Data Size in Kb	Execution Time in milliseconds		
	MD5 Algorithm	ARSM Algorithm (Proposed)	Difference in milliseconds
25	529	587	58
35	564	762	198
55	623	893	270
65	793	1498	705
85	1158	1533	375
95	1213	1728	515

Table-5. Comparison performance of encryption execution time MD5 and ARSM



Graph-5: Comparison performance of encryption execution time MD5 and ARSM.

It is refreshing to say that in the tested environment ARSM Algorithm has shown improved results in comparison with respected to other algorithms. Therefore the results obtained justify the proposed concept.

XIII. LIMITATIONS OF PRESENT STUDY

The present study has the aimed to study to find an optimal solution for Threat detection, prevention and effective defense mechanisms for the security in cloud. The present study is limited up to a hybrid hash algorithm (proposed) and a way to implement it. This study found that the existing AES, RSA, SHA-256 and MD5 algorithms have their own limitations. The limitations of these individual algorithms have driven to combine them. ARSM is a Hybrid hash algorithm with a combination of SHA-256, AES, RSA and MD5 algorithms. As per the analysis it is found effective over the considered other techniques.

DOI:10.22413/ijastems/2020/v7/i2/1

CONCLUSIONS

Cloud is a technically updating, sophisticated interactive collection of heterogeneous services under a single umbrella. Cloud technology has the problems with scheduling and balancing the load and the optimal computing resources utilization could solve the problem up to some level. Virtualization of cloud resources has brought some new challenges which are prone to get serious threats. There are many sorts of security mechanisms to secure the data. The aim of study is to find an optimal solution for Threat detection, prevention and effective defense mechanisms for the security in cloud using any hybrid hash algorithm and to implement. The present study has the aimed to study to find an optimal solution for Threat detection, prevention and effective defense mechanisms for the security in cloud.The present study is limited up to a hybrid hash algorithm (proposed) and a way to implement it . This study found that the existing AES, RSA, SHA-256 and MD5 algorithms have their own limitations. The limitations of these individual algorithms have driven to combine them. ARSM is a Hybrid hash algorithm with a combination of SHA-256, AES, RSA and MD5 algorithms. As per the analysis it is found effective over the considered other techniques.

Today much of the financial transactions are being performed online. There are many problems in crypto currency level. There is a need to check how well this present algorithm ARSM would bring any new improvements in terms of the existing problems like Spoofing payment information and phishing, Hacking a payment gateway, Insecure ICOs, Spoofing a user address etc.

ACKNOWLEDGEMENT

I sincerely I sincerely thank and express a deep sense of gratitude to my research supervisor Prof. T. Anuradha (Professor-in-Computer Science and Ex-Registrar and Ex -Vice-Chancellor (i/c) Dravidian University It could be impossible for me to present this paper without her patience in careful, thorough correcting and with her unprecedented methodologies phase in to create a pathfinder way, new innovative and gravitate ideas, mentorship for this paper.

REFERENCES

[1] S. Khan, A. S. Al-Mogren and M. F. AlAjmi, "Using cloud computing to improve network operations and management," 2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW), Riyadh, 2015, pp. 1-6, doi: 10.1109/NSITNSW.2015.7176418.

[2] Rao, G. and T. Anuradha. “Improved Hybrid Approach for Load Balancing In Virtual Machine.” (2018).

[3] I. Abbas, M. Ahmad, M. Faizan, W. Arshed and J. Khalid, "Issues and Challenges of Cloud Computing in Performance Augmentation for Pervasive Computing," 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 2020, pp. 1-7, doi: 10.1109/ICECCE49384.2020.9179462.

[4] G. Srinivasa Rao, T. Anuradha, “Improved Implementation of Hybrid Approach in Cloud Environment,” International Journal of Computer Sciences and Engineering, Vol.6, Issue.10, pp.254-260, 2018.

[5] E. A. Ahmed and H. Ali Ahmed, "A Proposed Model for Education System Using Cloud Computing," 2018 3rd International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), Karachi, Pakistan, 2018, pp. 1-4, doi: 10.1109/ICEEST.2018.8643331.

[6] Gundu, S.R., & Anuradha, T. (2019). Improved Hybrid Algorithm Approach based Load Balancing Technique in Cloud Computing. Global journal of computer science and technology.

[7] W. Ke, Y. Wang and M. Ye, "GRSA: Service-aware flow scheduling for cloud storage datacenter networks," in China Communications, vol. 17, no. 6, pp. 164-179, June 2020, doi: 10.23919/JCC.2020.06.014.

[8] Gundu, Srinivasa Rao. “Analytic Review of Mathematical model for non-linear programming problem formulation: A novel Queuing Theory approach using stochastic cloudlet request evaluation in cloud computing environment.” (2020).

[9] Srinivasa Rao Gundu, T. Anuradha, “Digital Data Growth and the Philosophy of Digital Universe in View of Emerging Technologies,” International Journal of Scientific Research in Computer Science and Engineering, Vol.8, Issue.2, pp.59-64, 2020.

[10] X. Zhu, L. T. Yang, H. Chen, J. Wang, S. Yin and X. Liu, "Real-Time Tasks Oriented Energy-Aware Scheduling in Virtualized Clouds," in IEEE Transactions on Cloud Computing, vol. 2, no. 2, pp. 168-180, April-June 2014, doi: 10.1109/TCC.2014.2310452.

[11] Srinivasa Rao Gundu, T. Anuradha, “Digital Data Growth and the Philosophy of Digital Universe in View of Emerging Technologies,” International Journal of Scientific Research in Computer Science and Engineering, Vol.8, Issue.2, pp.59-64, 2020.

[12] W. Sun, N. Zhang, H. Wang, W. Yin and T. Qiu, "PACO: A Period ACO Based Scheduling Algorithm in Cloud Computing," 2013 International Conference on Cloud Computing and Big Data, Fuzhou, 2013, pp. 482-486, doi: 10.1109/CLOUDCOM-ASIA.2013.85.

[13] Gundu, S.R., Panem, C.A. & Thimmapuram, A. RealTime Cloud-Based Load Balance Algorithms and an Analysis. SN COMPUT. SCI. 1, 187 (2020).

[14] W. Tian, Y. Zhao, Y. Zhong, M. Xu and C. Jing, "A dynamic and integrated load-balancing scheduling algorithm for Cloud datacenters," 2011 IEEE International Conference on Cloud Computing and Intelligence

Systems, Beijing, 2011, pp. 311-315, doi: 10.1109/CCIS.2011.6045081.

[15] Gundu, S.R., Panem, C.A. & Thimmapuram, A. Intelligence Using Automata-Based Nature's Digital Philosophy. SN COMPUT. SCI. 1, 189 (2020).

[16] N. Jain and S. Choudhary, "Overview of virtualization in cloud computing," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-4, doi: 10.1109/CDAN.2016.7570950.

[17] V. Meena, V. Arvind, P. Vijayalakshmi, V. Kalpana and J. S. Kumar, "Optimized task clustering for mobile cloud computing using Workflowsim," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 2018, pp. 1000-1005, doi: 10.1109/ICISC.2018.8398952.

[18] W. Ben Slama, Z. Brahmi and M. M. gammoudi, "Interference-Aware Virtual Machine Placement in Cloud Computing System Approach Based on Fuzzy Formal Concepts Analysis," 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Paris, 2018, pp. 48-53, doi: 10.1109/WETICE.2018.00016.

[19] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges," in IEEE Access, vol. 8, pp. 3343-3363, 2020, doi: 10.1109/ACCESS.2019.2962829.

[20] T. Wang, Z. Su, Y. Xia and M. Hamdi, "Rethinking the Data Center Networking: Architecture, Network Protocols, and Resource Sharing," in IEEE Access, vol. 2, pp. 1481-1496, 2014, doi: 10.1109/ACCESS.2014.2383439.

[21] Gundu, S.R., Panem, C.A. & Thimmapuram, A. "The Dynamic Computational Model and the New Era of Cloud Computation Using Microsoft Azure". SN COMPUT. SCI. 1, 189 (2020). doi.org/10.1007/s42979- 020-00276-y

[22] Gundu, S.R., Panem, C.A. & Thimmapuram, A. "Hybrid IT and Multi Cloud an Emerging Trend and Improved Performance in Cloud Computing". SN COMPUT. SCI. 1, 189 (2020). doi.org/10.1007/s42979-020-00277-x

[23] P. Harsh, F. Dudouet, R. G. Cascella, Y. Jegou and C. Morin, "Using open standards for interoperability issues, solutions, and challenges facing cloud computing," 2012 8th international conference on network and service management (cnsm) and 2012 workshop on systems virtualiztion management (svm), Las Vegas, NV, 2012, pp. 435-440.

[24] L. Ogiela, M. R. Ogiela and U. Ogiela, "Cognitive information systems in secure information management and personalized cryptography," 2014 Joint 7th International Conference on Soft Computing and Intelligent Systems (SCIS) and 15th International Symposium on Advanced Intelligent Systems (ISIS), Kitakyushu, 2014, pp. 1152-1157, doi: 10.1109/SCIS-ISIS.2014.7044798.

[25] X. Zhang, R. WU, M. Wang and L. Wang, "A High-Performance Parallel Computation Hardware Architecture in ASIC of SHA-256 Hash," 2019 21st International Conference on Advanced Communication Technology (ICACT), PyeongChang Kwangwoon_Do, Korea (South), 2019, pp. 52-55, doi: 10.23919/ICACT.2019.8701906.

[26] F. Kahri, H. Mestiri, B. Bouallegue and M. Machhout, "Efficient FPGA hardware implementation of secure hash function SHA-256/Blake-256," 2015 IEEE 12th International Multi-Conference on Systems, Signals & Devices (SSD15), Mahdia, 2015, pp. 1-5, doi: 10.1109/SSD.2015.7348105.

[27] Y. Yuan, Y. Yang, L. Wu and X. Zhang, "A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation," 2018 IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC), Shenzhen, 2018, pp. 1-2, doi: 10.1109/EDSSC.2018.8487056.

[28] P. Deshmukh and V. Kolhe, "Modified AES based algorithm for MPEG video encryption," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, 2014, pp. 1-5, doi: 10.1109/ICICES.2014.7033928.

[29] P. Deshmukh and V. Kolhe, "Modified AES based algorithm for MPEG video encryption," International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, 2014, pp. 1-5, doi: 10.1109/ICICES.2014.7033928.

[30] M. Bahadori, M. R. Mali, O. Sarbishei, M. Atarodi and M. Sharifkhani, "A novel approach for secure and fast generation of RSA public and private keys on SmartCard," Proceedings of the 8th IEEE International NEWCAS Conference 2010, Montreal, QC, 2010, pp. 265-268, doi: 10.1109/NEWCAS.2010.5603937.

[31] Y. Wu and X. Wu, "Implementation of efficient method of RSA key-pair generation algorithm," 2017 IEEE International Symposium on Consumer Electronics (ISCE), Kuala Lumpur, 2017, pp. 72-73, doi: 10.1109/ISCE.2017.8355552.