A review for new scenario for providing Security for Data Migration using combinationof ECC & MAES Algorithms.

Mer Utsav H.[1], Mr. Nimit Modi[2], Dr. Sheshang D. Degadwala[3]

[1]*PG student,Computer Engineering Department, SigmaInstitute of Engineering, Vadodara, Gujarat, India, merutsav95@gmail.com*

[2]*Assistant Professor,Computer Engineering Department, Sigma Institute of Engineering, Vadodara, Gujarat, India, nimit.cs.engg@sigma.ac.in*

[3]*Head Of the Department, Computer Engineering Department,Sigma Institute of Engineering, Vadodara, Gujarat, India, sheshang13@gmail.com*

ABSTRACT

Data migration is the process of transferring data between computers, client storage to server storage devices or formats or to cloud. Data can be of any form audio, video or images. So basically, data is the main concern for today's highly technological and virtual world. So, it is very important that whatever data is being migrate remain safe and highly optimized. So, this paper is about providing security to data while it's migration from the client to storage or to storage to the source using cryptography mechanism. In cryptography mechanism we've used ECC Cryptography. ECC requires smaller keys compared to non-EC cryptography to provide equivalent security. Also, we've used MAES to provide more security and overcome the disadvantages of ECC.Also, optimization and better selection of data increases its usefulness and decreases risks like availability, performance, portability, integrity, adaptability etc. For that we've shown a trust mechanism which will run before data migration for data validation. Trust is a critical factor in cloud computing; in present practice it depends largely on perception of reputation, and self-assessment by providers of cloud services. Here we've used behavior, query validation, threshold, data validation, verification, reliability etc. as parameters of trust mechanism. So we've worked on data validation, data security & data migration between client to storage, storage to source, between computers, or data migration in cloud.

Keywords: *-Data migration, ECC, Data validation, Data security, Trust mechanism, MAES, Elliptic curve cryptography, modified advance encryption standards.*

---

1. INTRODUCTION:

Cloud computing is shared pools of configurable computer system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a public utility. Cloud computing is the use of various services, such as software development platforms, servers, storage and software, over the internet, often

referred to as the "cloud." Many cloud computing advancements are closely related to virtualization. The ability to pay on demand and scale quickly is largely a result of cloud computing vendors being able to pool resources that may be divided among multiple clients.[12]

Data migration is the process of transporting data between computers, storage devices or formats. In context of cloud computing Data migration is the process of moving data, applications or other business elements to a cloud computing environment.[12]

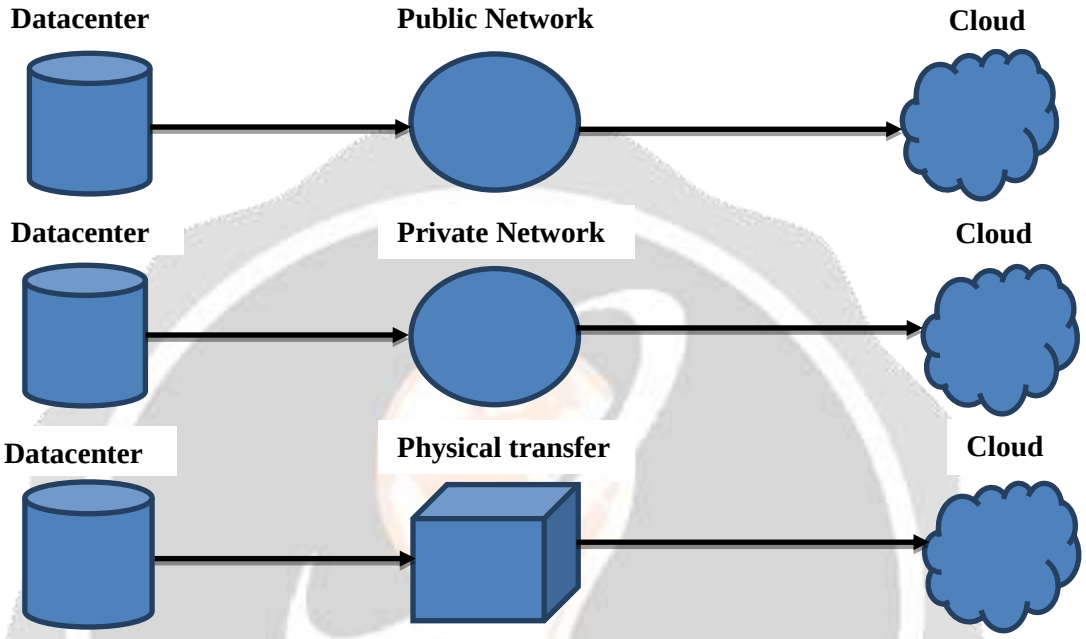

Figure 1 Data migration to cloud.

When we are thinking about cloud computing security is a highly critical problem and demands a must attention as every single day new kinds of security attacks are coming and security risks for data in cloud increasing rapidly. When it comes to Network security, In the recent months, aggressive marketing by various Cloud providers have made it easier for hackers to get accounts and plant botnets. Cloud is also susceptible to a lot more Denial of Service attacks. Cloud Providers need to ensure that their perimeter is secure and barrier to attacks is high. So here we are providing security for data migration in cloud using combination of MAES & ECC algorithms.[12]

2. CRYPTOGRAPHY:

Cryptography is the art and science of protecting information from unwanted person and converting it into a form undistinguishable by its attackers though stored and transmitted. The main aim of cryptography is keeping data secure form unauthorized persons. Data cryptography mostly is the scramble of the content of data, such as text data, image related data and audio, video related data to compose the data illegible, imperceptible or unintelligible during communication or storage called Encryption process. The reverse of data encryption process is called data Decryption. [11] Modern cryptography concerns with:

Confidentiality - Information cannot be understood by anyone.

Integrity - Information cannot be altered.

Non-repudiation - Sender cannot deny his/her intentions in the transmission of the information at a later stage.

Authentication - Sender and receiver can confirm each.

Information security uses cryptography on several levels. The information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. Cryptography also aids in nonrepudiation. This means that the sender and the delivery of a message can be verified.

Important Terms of Cryptography:

Figure 2 Cryptography System.

Some of the common terms that are used in cryptosystems are explained here.

Plaintext - This is the original intelligible message or data that is fed into algorithm as input.

Ciphertext - The encoded message send to other side over network.

Encryption - The method of producing cipher text from plaintext using the key is called as Encryption.

Decryption - The reverse procedure of producing the plaintext from cipher text using the key is called as Decryption.

Cryptanalysis – It is the study of how to know encryption algorithms or their implementations.

Types of cryptography:

- **Symmetric Key Cryptography** – Here only one key is used for both encryption and decryption. This type of encryption is also referred to as Secret Key Cryptography (SKC).

- **Asymmetric Key Cryptography**-Here two keys are used. One key is the public key that anyone can access. The other key is the private key, and only the owner can access it. Also called Public Key Cryptography (PKC).

Data security is the challenging issue of today that touches many areas including computersand communication.Modern cyber security attacks have surely played with the effects of theusers. Cryptography is one such technique to create certain that, authentication, integrity,availability, confidentiality and identification of user data can be maintained as well assecurity and privacy of data can be provided to the user. The cryptography techniques andvarious algorithms are used to provide the needed security to the applications.

Since the security challenges are increasing day-by-day in the cloud computing environment and the privacy of clients is at risk as the data is transferred from one cloud to another cloud during the migration process. The security of data has become the major issue in cloud environment. Here we focused in improving the data security with the randomized encryption technique.

3. PROPOSED SYSTEM:

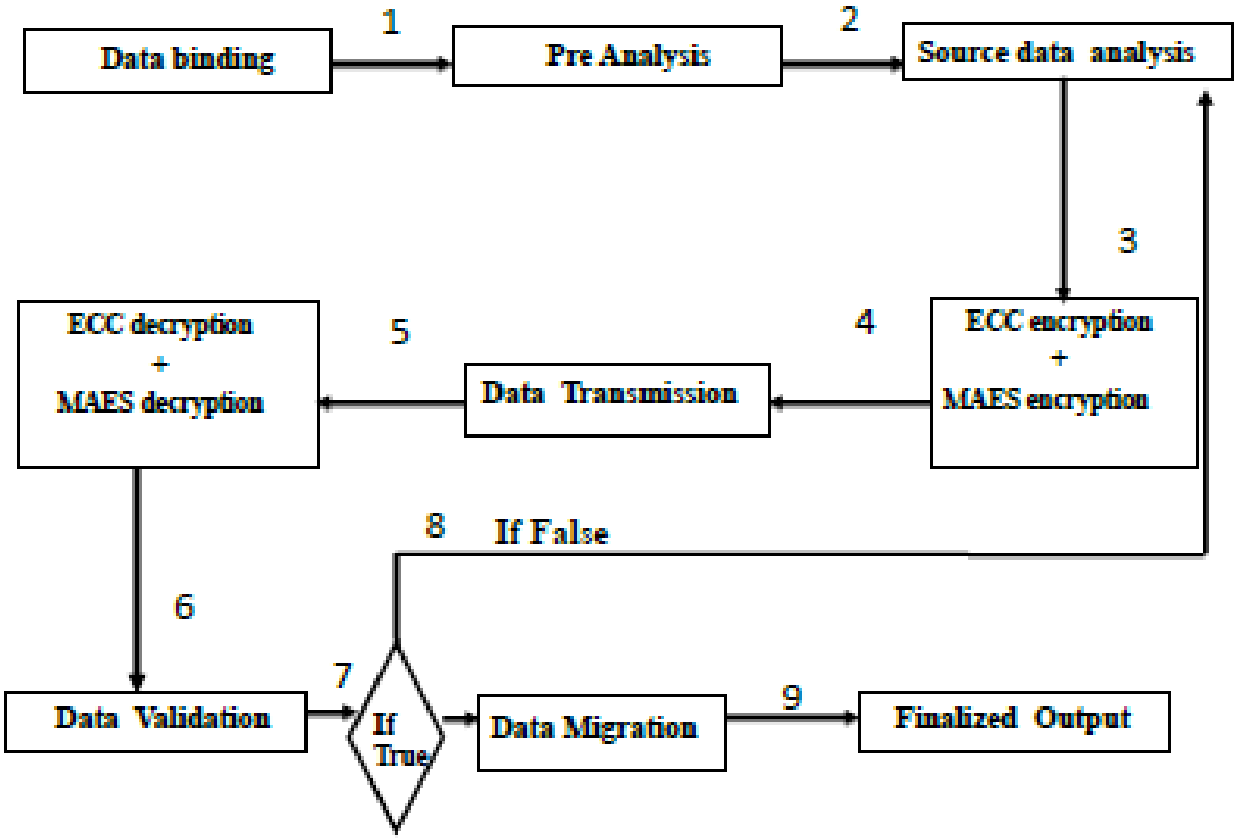

Figure 3 Proposed Work.

Proposed Work: In my proposed work, a new technique of security is presented using combination of ECC & MAES algorithms with trust mechanism for optimization of data.

Data Binding: The process of collecting raw data from environment.

Pre-Analysis: This is basically the process of data classification and arraigning the data in differentclass where itbelongs.

Source data analysis: To decide which data is important, basically selecting right data and loading it to the database or data storage.

ECC + MAES Encryption: Encrypting the data using ECC+MAES algorithms which has been chosen for data transformation from database according to the request ordemand of user or service provider or anyone else.

Data Transformation: The process of transforming data from sender or source to receiver or desireddestination using data communication system in cloud.

ECC + MAES Decryption: Decrypting the data which have received at destination after being transformed from sender using ECC + MAES algorithm.

Data Validation: It is the process of validating data, basically checking that is the received data issame as it has been sent from sender or data is being compromised during datatransformation.If the data passes all the parameters of data validation it will be sent for data migration if not than will be sent to source data analysis for re-transformation.

Data Migration: It is the method of moving a large amount of data and applications into the target cloud where the target cloud can be – a public, a private or hybrid cloud.
Finalized Output: When data migration successfully done and data has been migrated to desired location.

4. LITERATURE SURVEY:

4.1 Secure keyword search using dual encryption in cloud computing.

Husna Tariq, ParulAgarwa (2018) have proposed a system for the secure searching, stockpiling and recovery of client information in the cloud framework. Different services of cloud, security issues and security necessities of cloud information being talked about. We have utilized fuzzy keyword searching scheme to seek and recover the encrypted data. The limitations are They have used RSA so it will take large number of bits for encryption so it's time consuming also less secure because hybrid approach is not used. Only 1 algorithm is there to provide security so comparatively less secure. [1].

4.2Velocity-Aware Parallel Encryption Algorithm with Low Energy Consumption for Streams.

Xiongwei Fei, Kenli Li, Senior Member, IEEE, Wangdong Yang, and Keqin Li, Fellow, IEEE (2017) have proposed a velocity-aware parallel encryption algorithm with low energy consumption (LECPAES) for streams in cloud computing. The algorithm parallelizes Advanced Encryption Standard (AES) based on heterogeneous many-core architecture, adopts a sliding window to stabilize burst flows, senses the velocity of streams using the thresholds of the window computed by frequency ratios, and dynamically scales the frequency of Graphics Processing Units (GPUs) to lower down energy consumption. The experiments for streams at different velocities and the comparisons with other related algorithms show that the algorithm can reduce energy consumption. The limitations are Same key used for encryption at both side and the main disadvantage is it can be used only for stable data streams with fixed inflow speed. Can't handle complicated data stream. [2].

4.3 An ultra-high throughput and fully pipelined implementation of AES algorithm on FPGA.

Ali Abdulridha Taha, Diaa Salama Abd Elminaam and Khalid M. Hosny (2015) propose area-delay efficient multipliers and multiplicative inverters in GF. They employ loop-unrolling, fully pipelining, and sub-pipelining techniques in all proposed methods. Moreover, They insert registers of pipelining in optimal placements. These reasons demonstrate that proposed methods not only try to keep the advantages of previous works but also try to decrease their disadvantages. The limitation is that it is Very complicated to implement and both side same key used as only AES is used. [3]

4.4 Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile data to Cloud.

Sujithra Ma, Padmavathi G , Sathya Narayanan (2015) In the technology up-front world, mobile devices like smartphones and tablets are inevitable. When computing capacity and storage need of these devices are increasing tremendously, it demands the secure way of storing the data in cost efficient model. This paper describes how securely the mobile data can be stored in the remote cloud using cryptographic techniques with minimal performance degradation. The limitation is that So many algorithms are used so time complexity of the model is very high and also parameters like throughput and turn around time not taken in consideration. [4]

4.5 A resource-efficient encryption algorithm for multimedia big data.

ShadiAljawarneh& Muneer Bani Yassein&We'am Adel Talafha (2017) have discussed approaches and evaluate the popular ones in order to find the elements that affect system performance. Finally, they will propose a model that enhances data security and privacy by combining Advanced Encryption Standard-256, Information Dispersal Algorithms and Secure Hash Algorithm-512. Their protocol achieves provable security assessments and fast execution times for medium thresholds. The limitation is that Only AES is used for encryption that's why robust compare to other hybrid approach and same key used for encryption and decryption. [5].

4.6A Secure CloudComputing Model based on Data Classification.

Lo'ai Tawalbeh1, Nour S. Darwazeh, Raad S. Al-Qassas and Fahd AlDosari (2015) proposed a secure cloud computing model based on data classification. The proposed cloud model minimizes the overhead and processing time needed to secure data through using different security mechanisms with variable key sizes to provide the appropriate confidentiality level required for the data. The proposed model was tested with different encryption algorithms, and the simulation results showed the reliability and efficiency of the proposed framework. The limitation is tha Only encrypts confidential data and only symmetric algorithms are used. [6].

4.7Secured User's Authentication and Private Data Storage- Access Scheme in Cloud Computing Using Elliptic Curve Cryptography.

Shilpi Singh Vinod Kumar (2015) propose a scheme that not only provides security of user's private data of storing and accessing over the cloud but also authentication of the user to the cloudserver using Elliptic curve cryptography. The limitations are that only For data encryption symmetric algorithm is used and there is no provision of data optimization. [7].

4.8Integrated ECC and Blowfish for Smartphone Security.

Payal Patel, Rajan Patel, Nimisha Patel (2016) develop the scheme to secure the mobile data in cloud using cryptography, in which Elliptic Curve Cryptography and Blowfish algorithm are integrated to provide authentication and confidentiality. To transmit the data more securely, random number is used to increase computational complexity for an adversary. We also randomize the number of rounds of Blowfish for performance improvement. Their approach is implemented and tested with different platforms like personal computer, android emulator, smartphone and aakash tablet. The limitation is that the combination of ECC and Blowfish is used which is less secure than combination of MAES & ECC. Also they've set minimum rounds of blowfish as 5, where in AES you will get it as 16 so less secure compared to our proposed system. [8].

4.9Secure Sharing and Searching for Real-Time Video Data in Mobile Cloud.

Joseph K. Liu, Man Ho Au, Willy Susilo, Kaitai Liang, Rongxing Lu, and Bala Srinivasan. (2017) an infrastructure that allows mobile users to securely share and search for their real-time video data. Specifically, the proposed infrastructure takes the advantages of the cloud platform and 5G technology to achieve its goals, where mobile users

(connected with some external video taking device) can share their real-time video with their friends or families through the cloud while any other user with no permission cannot get any information about the video. More importantly, the infrastructure security is guaranteed even if the cloud server is hacked. In addition, our infrastructure also allows secure searching within the user's own video data. We believe our solution is practical to be deployed in the existing telecommunication platforms. The limitation is they Only provide security for video data in mobile cloud, not provided security scheme for all kinds of data. [9]

4.10Fast Cloud-RSA Scheme for Promoting Data Confidentiality in the Cloud Computing.

Khalid El Makkaouia, Abderrahim Beni-Hssaneb, AbdellahEzzatia, Anas El-Ansarib (2017) propose a new fast variant of the Cloud-RSA scheme to speed up its algorithms. The proposed variant uses a modulus of the form N = prqs for r, s ≥ 2 and employs Hensel lifting and Chinese remaindering to decrypt. Simulation res results show that the proposed variant gives a large speed up over the Cloud-RSA scheme while preserving a prescribed security level.The limitation is They have used only RSA algorithm for security, it is complex and time taking as large prime numbers are used also less secure because hybrid approach is not used. Only 1 algorithm is there to provide security so comparatively less secure. [10]

5. CONCLUSION:

As we can see from comparison table of algorithms the combination of ECC & MAES gives best result to provide security for data migration in cloud computing. As this is a combination of Symmetric and Asemantic key algorithms, they fulfill the lack of each other and provide a robust system. Reason for ECC can use smaller keys for the same level of security, Very fast key generation, Fast signatures, Moderately fast encryption and decryption, MAES is used for strongly secure transmission of data. Modification of AES makes it more efficient and secure because here shiftrow operation get modifies so we will get more strongly encrypted data. Also, AES and MAES comparison is shown, MAES is less time consuming and less complex than AES. Overall this model is an optimum solution for security for data migration in cloud computing.

6. REFERENCES:

[1] "Secure keyword search using dual encryption in cloud computing."Husna Tariq, ParulAgarwa, Springer 2018.

[2] "Velocity-Aware Parallel Encryption Algorithm with Low Energy Consumption for Streams." Xiongwei Fei, Kenli Li, Senior Member, IEEE, Wangdong Yang, and Keqin Li, Fellow, IEEE IEEE Transaction 2017.

[3] "An ultra-high throughput and fully pipelined implementation of AES algorithm on FPGA." Ali Abdulridha Taha, Diaa Salama Abd Elminaam and Khalid M. Hosny Elsevier 2015.

[4] "Mobile Device Data Security: A Cryptographic Approach by Outsourcing Mobile data to Cloud."Sujithra Ma, Padmavathi G , Sathya Narayanan Elsevier 2015.

[5] "A resource-efficient encryption algorithm for multimedia big data." ShadiAljawarneh& Muneer Bani Yassein&We'am Adel Talafha Springer 2017.

[6] "A New Security Protocol Using Hybrid Cryptography Algorithms." Yasmin Alkady, Mohmed I. Habib, Rawya Y. Rizk IEEE 2013.

[7] "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" Gurpreet Singh,Supriya. IEEE 2013.

[8] "MAES: Modified Advanced Encryption Standard for Resource Constraint Environments" Arnab Rahman Chowdhury, unayedMahmudy, Abu Raihan MostofaKamaly, Md. Abdul hamid IEEE 2018.

[9] "An Efficient Modified Advanced Encryption Standard (MAES) Adapted for ImageCryptosystems"Internationljournal of computer science Abdulkarim Amer Shtewi†, BahaaEldin M. Hasan, Abd El Fatah .A. Hegazy

[10] "An Improved AES-ECC Hybrid Encryption Scheme for Secure Communication in Cooperative Diversity based Wireless Sensor networks." Anirudh Ramaswamy Ganesh, Naveen Manikandan ,Sethu S, Sundararajan , Pargunarajan IEEE 2017

[11] "Comparative Study of Symmetric and Asymmetric Cryptography Techniques." Ritu Tripathi1, Sanjay Agrawal, International Journal of Advance Foundation and Research in Computer (IJAFRC)-2014.

Reference Websites:

[12] https://en.wikipedia.org/wiki/Cloud_computing

[13] https://searchcloudcomputing.techtarget.com/definition/cloud-migration

[14]https://searchsecurity.techtarget.com/definition/cryptography

7. AUTHORS PROFILE:

Mr. Mer UtsavH. has completed his bachelor from Shantilal shah engineering collage, in 2016. His area of interest isCloud computing. Working on Security for data migration in cloud. Pursuing master in computer engineering from Sigma institute of engineering,

Dr. Sheshang D. Degadwala Completed Ph.D. in Computer Engineering from Madhav University, Abu Road, Sirohi, Rajasthan, India in year 2018. He is currently working as Head of Computer Engineering Department in, Sigma Institute of Engineering, Vadodara, India since 2012. He has published more than 58 research papers in reputed international journals and 3 in National conferences including Thomson Reuters and conferences including IEEE, Springer and it's also available online. His main research work focuses on Image Processing, Information Security and Data Mining. He has 6 years of teaching experience and 6 years of ResearchExperience.

Mr. Nimit Modi, Assistant Professor Department of Computer Engineering ,Sigma Institute of Engineering,Vadodara,Gujarat. B.E in Computer Engineering 2010 M. E in Computer Engineering -2013 Published 6 research paper in IJSRSET journals and conference Area of interest :Mobile ad-hoc network and wireless communication, cloud computing.