Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

A Review on Performance of Online Transaction Algorithms in Cloud Environment

Manju Subashini[1]
[1] UG Scholar, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram- 605108.

Prabakaran D[2]
[2]AssociateProfessor, Department of Electronics and Communication Engineering, IFET College of Engineering, Villupuram- 605108.

***Abstract*— The cloud computing is a infrastructure technology that provides access to users over internet. The users with their sensitive credentials, gains access to the cloud service on successful verification of authentication credentials. The security issues in cloud computing proves to be a run back process deteriorating the performance of cloud computing. This paper proposes a model that integrates the traditional authentication method with Hashing algorithm and performing a secured encryption using Elliptical Curve Cryptography (ECC).This model evades and addresses the security issues in cloud computing.**

Keywords: Authentication, Cloud computing, Elliptical Cloud Cryptography, Hashing.

1. INTRODUCTION:

Cloud computing means storing and accessing data over internet instead of computer's hard drive. The cloud contains all the data of the user and it can be accessed via the internet across the globe. The Cloud computing is an emanating technology that is being used by common people to the IT professionals. Broad network access, elasticity, resource pooling, measured service are the prominent characteristics of cloud computing. The Cloud computing is increasingly used in big data analytics, file storage, disaster recovery, e-commerce websites and business processing. Digital money transfer is one of the esteemed applications of cloud computing. This is facilitated by the user by providing legitimate authentication details via mobile phone device or computer. This digital exchange is started on the user's device routed via cloud proxy server to the destinated banking server. Thus, safeguarding the confidential information stored on the cloud has become crucial. As a matter of security, a static one-time authentication measures such as PINs and then patterns were introduced. But the probability of brute forcing the PIN, pattern was high. Next, authentication using finger prints was implemented, but complete data security was unable to achieve. Then, an One Time Password (OTP) authentication was introduced. Here, when an authenticated user requests for service from the cloud, an OTP of 4 to 6 digits will be sent to the registered e-mail or mobile number by the user. When the correct OTP is entered, the requested service will be provided by the cloud otherwise service would be denied by the cloud. Precisely, the OTP is used for the confirmation of identity of the user. This ,two factor authentication is seemed to be efficient but, they are easily prone to shoulder surfing attacks and smudge attacks. This project proposes a three factor authentication which comprises of password, OTP and weighted pattern product. This project aims in providing a secure and adaptable authentication mechanism based on not only what the user inputs but also on the pattern of the otp. An important characteristic of behavioral authentication is that the probability of being hacked/stolen is limited than others device.

2. CLOUD COMPUTING SERVICES:

The three different service models in cloud computing are Saas, Paas, Iaas.

The first service is Software as a software (SaaS) concerns with web based services.Saas offers complete service application to end customers based on demand. Google, Microsoft, Sales force offer this Saas in the current scenario.

The second service is Infrastructure as a software (Iaas)is an instant computing infrastructure facilitates virtualized computing resources via insecure internet.Iaas users contact cloud resources via Wide Area Network(WAN).Iaas is easier, faster and cost efficient.Iaas offers pay as you go to model which does not involve any capital expense in deploying an infrastructure. Amazon, 3 Tera, GoGrid are some commonly used Iaas

The third service is Platform as a Service (PaaS) which provides more freedom to users in selecting the computing platform which they want to use. The user need to manage the platform and the service providers offers a predefined combination of operating System and application servers. Google App Engine, Force.Com, Azure are some of the common examples of PaaS.

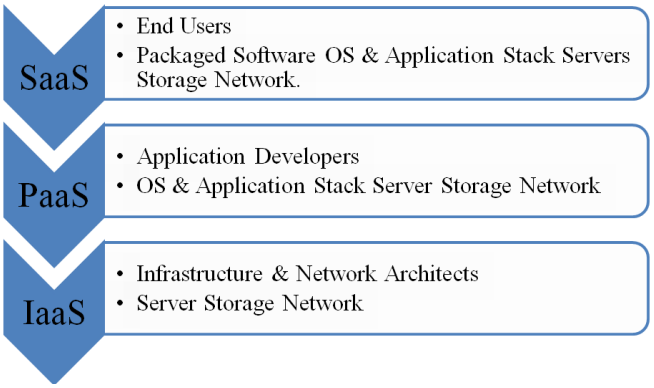

Fig: 1: Cloud service models

Other classifications of cloud are:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

- **Public Cloud**: Any organization may give service available visibly.
- **Private Cloud**: Service can be handy only inside a private network.

3. ONLINE TRANSACTION BENEFITS

Cloud computing service became popular in day to day life due its following notable pros.

Increased Speed and Convenience

We can pay for things or services online at any time of day or night, from any corner of the world. We need not have to spend time in a line, waiting to pay the bill.

Reduced labour costs

The online payments are generally automatic. They have reduced labour costs than hand operated payment methods, such as cheque, money order, and cash.

Back-up and restore data:

Once the data is hoarded in a Cloud server, it is apparent to get the back-up and recovery of that data, which is much very time consuming process.

Automatic Software Integration:

Software integration occurs automatically in online transaction. Therefore, we don't need to take supplementary efforts to adapt and incorporate our applications as per our preferences.

Reliability:

Reliability is one of the biggest dominance of online transaction. We can always get instantaneous updates regarding the changes.

Portability:

Employees who are working on remote locations can effortlessly transfer money to any location. All they necessitate is an Internet connectivity.

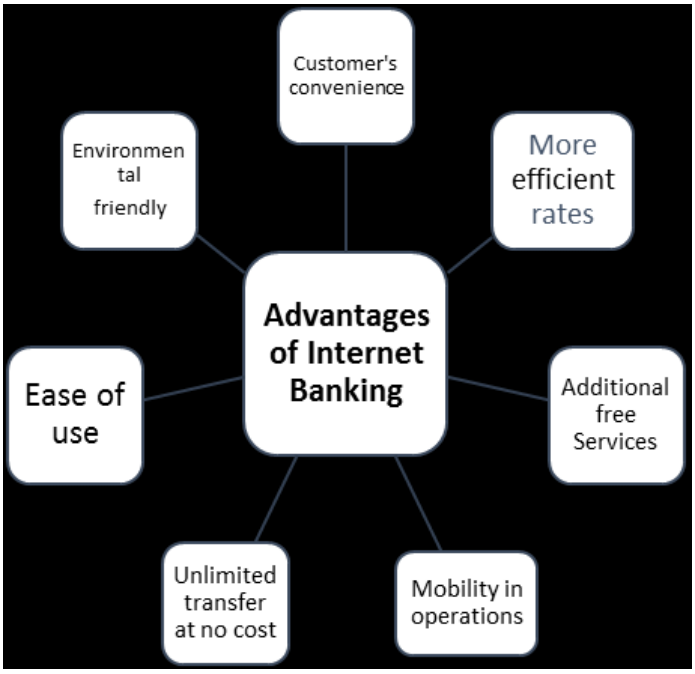

Fig: 2: Advantages of Online transaction

4. ISSUES IN ONLINE TRANSACTIONS:

Risk to e-commerence:

E-Commerce cites to the action of exchanging things through the internet. It refers to the business transactions which are conducted online .E-commerce threat is stirring by using internet for iniquitous means with the objective of stealing, scam and security infringe. There are various types of e-commerce threats. The most widespread security risks are an electronic payments system, e-cash, data exploitation, credit/debit card frauds, etc.

Electronic payment scheme:

With the swift advancement of computer, mobile, and network technology, e-commerce has become habitual in human life. E-commerce organizations use electronic payment systems that use paperless monetary transactions. It has a vast threat of scam if the computing devices exercise identity of the person for authorizing a payment such as passwords and security questions.

Hazard of tax dodging:

The Internal Revenue Service law states that every business should disclose their financial transactions and present paper records so that tax acquiescence can be substantiated. The crisis with electronic systems is that they don't present cleanly into this concept. The IRS does not whether the disclosed records are true which makes It trouble-free to dodge taxation.

E-cash:

E-cash is a paperless cash method which simplifies the transfer of finances incognito. Pay Pal, Google Pay, Pay tm are the common examples of e-cash system

E-cash has four major components- Issuers, Customers, Traders, Regulators

E-cash risks:

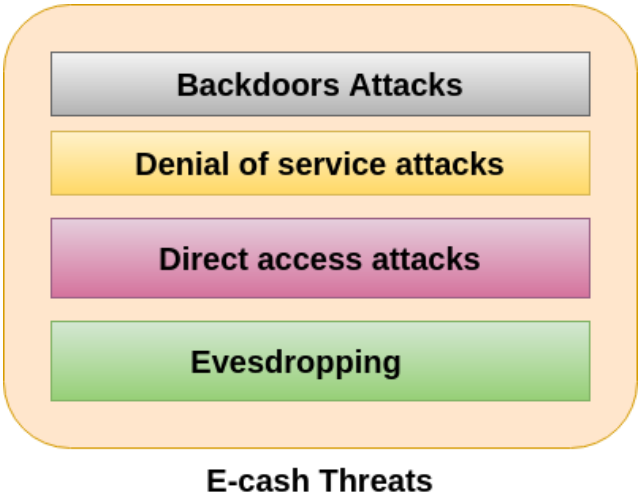

Fig 3: E – cash Threats

Backdoors Attacks:

An attacker to illegally admittances into a system bypassing the regular validation mechanisms is known as backdoor attack.. It works in the background and masks itself from the user that makes it tricky to sense and eliminate.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

Denial of service attacks:

A defense attack in which the attacker performs certain action that impedes the legitimate users from pervading the electronic devices is known as denial of service attacks. It makes a system source occupied to its deliberate users by momentarily distracting services of a host linked to the Internet.

Direct Access Attacks:

Direct access attack is an attack in which an attacker acquires substantial access to the computer to carry out an illegal activity and installing assorted types of software to copout security. The software are encumbered with worms and download a huge sum of susceptible data from the target victims.

Eavesdropping:

Eavesdropping is an unlawful way of heeding to confidential communication over the network. It does not obstruct with the ordinary operations of the targeting system. So the sender and the receiver of the messages will not be aware that their conversation is being tracked.

Man in middle attack:

A malicious attacker infuses him/herself into a conversation between sender and receiver, mimics both and gains admittance to data that the two parties were trying to forward to each other. The attacker may abduct login credentials or any personal data, scout on the victim, or interrupt communications or corrupt data.

Identity thefts:

The identity theft refers to unauthorized exploitation of someone's individual data or documents to acquire products or services. Data breaches can unmask our personal data and depart defenseless. Offline methods also add on to the extenion of identity theft.

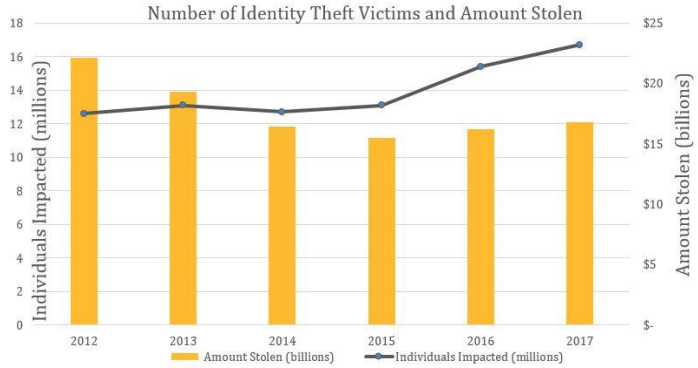

Fig 4: Identity thefts and the amount stolen

Targeted attacks:

The main aim of target attack is to break into the target's network and strip information from the servers. Majority of the target attacks are habitually state-sponsored, however some have been by confidential groups.

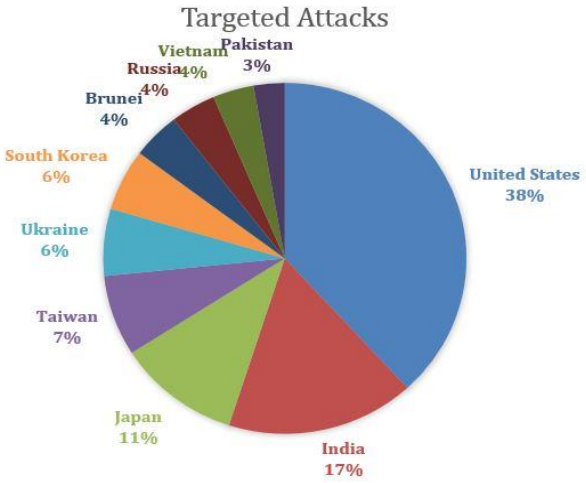

Fig: Targeted attacks in various countries

5. SECURE ONLINE TRANSACTIONS- A REVIEW

The demands for cloud computing service are very much escalating due to its remarkable merits, followed by the demerits like security concerns still exists. Numerous research are being done to surmount the security issues in cloud computing. The Cloud Security Alliance (CSA) is a society furnishes existing and impending challenges in cloud computing and also produce legitimate solutions for the same. The universally accepted cloud computing standards are proclaimed by this society. Intel and IBM are some of the eminent organizations participating in open debate to offer and uphold cloud security solutions. The Open Web Application Security Project (OWASP) find the security threats in cloud services. The discussion yields a solution of designing a framework with tough security architecture. A survey has been conducted on the possible solutions for the security threats of cloud computing and is listed here.

Rajendra Patil et al. in 2019 implemented a hypervisor level distributed network security (HLDNS) framework [1] which is deployed on each processing server. At each server, it monitors the underlying virtual machines related network obtrusion. The extension of binary bat algorithm provides two new fitness functions for deriving feasible features from cloud network traffic.

Zahed Syed et al. in 2018 demonstrated that the user's posture, device size and configuration have a significant impact on the performance of touch-based authentication Systems [2]. A new public data set of protocol controls was created. He concluded that the Authentication accuracy increases with the device size. At the same time, current state-of-the-art attributes cannot authenticate across changes in device size or screen orientation.

Milad Taleby Ahvanooey et al. in 2018 proposed a innovative text steganography technique [3] called AITSteg.It provides end-to-end security during the transmission of text messages via SMS between end users. The embedding capacity, invisibility, robustness, and security were evaluated in this approach. This AITSteg is able to prevent various security issues like man-in-the-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

middle attacks, message disclosure, and manipulation by readers.

Joseph Gualdoni et al. in 2017 proposed Secure Online Transaction Algorithm (SOTA) [4] a explores to use two-factor authentication with the arbitrary codes. It uses mobile devices to log into card accounts through an application to prospect the arbitrarily originated code. This SOTA forms an extra layer of security that would anticipate hackers from probably impairing someone both financially and pensively.

Naga Hemanth et al. in 2017 designed a three stage algorithm [5] to provide an extra layer of security. The first stage includes encryption of text using playfair cipher of 9x6 matrixes. In the second stage, XOR operation is performed between the encrypted text and the encrypted key. By using RSA algorithm continued with a XOR operation between the encrypted text and the encrypted key is done at the final stage. Then the final encrypted text and the new encrypted key is decrypted by the receiver.

Jolanda Modica et al. in 2016 developed a modernistic cloud security estimation technique called Moving Intervals Process (MIP) [6] that can hold many requests in parallel.MIP offers accuracy and high computational efficiency. In this approach, by curbing the time required to rank CSP (Cloud Service Providers) according to the CSC (Cloud Service Customers) requirements, the CSCs are able to accustom their requests and perform assessment vehemently.

Siddaram K Jamagav et al. in 2016 framed an innovative method which adopts a light weight trapdoor compression method, [7] which reduces the trapdoor's size and increases the transmission rate. This scheme uses two methods to augments data search by using Trapdoor mapping table (TMT) and Ranked Serial Binary Search (RSBS) algorithm to accelerate the document revival time hence run over the communication latency and connectivity obstacles.

Bin Chen et al. in 2016 designed a physical layer security access called original symbol phase rotated (OSPR) secure transmission scheme [8] to insure against eavesdroppers armed with indefinite antennas. The basic concept of the proposed OSPR scheme is to inconstantly rotate the phase of original symbols at the base station (BS) before they are transmitted, so that the massive MIMO eavesdropper will be puzzled by the short stopped signals which may not enact the true information symbols.

Asma Salem et al. in 2016 proposed a framework which examines the keystroke dynamics and it uses this as a second factor of authentication. This framework [9] proposes a application for collecting timing and non timing information from keystroke dynamics. This achieves lower error rate of false acceptance, false rejection of and equal error rate.

Preeti Daffu et al. in 2016 implemented a security layer between the server end and the cloud user for secure data transmission over internet [10]. A Key exchange was implemented to provide a steady security in the cloud and to extenuate the security risks related to the cloud users. The encryption process rises the data size, this can be restrained by employing the compression technique over the encrypted data.

R. Pragaladan et al. in 2016 used the Watson-crick Hoogsteen base Confidential Data Transaction (WHO-CDT) Mechanism [11]to upgrade data seclusion. It demonstrated that confidentiality of data to be enhanced by utilising the DNA-based Ultra Compact Transactional information Storage where transactional data is transformed to binary storage using DNA sequence. The application of Oligonucleotide Sequences based Transactional Data Encoding and Decoding proves that WHO-CDT provides analogously insignificant execution time and hence enhances data confidentiality.

Kamal Kumar Chauhan et al. in 2015 designed a homomorphic encryption technique [12] in cloud computing to secure data in processing stage itself. It allows the users to operate encrypted data without any decryption. The homomorphic encryption helps to protect the integrity of the user's data. It was concluded that fully homorphic method took large time to operate on encrypted data.

Preeti Chandrasekhar et al. in 2015 proposed a RSA based secure and effective two-factor remote user authentication scheme, [13] which accomplishes mutual authentication and user invisibility properties. This proposed framework is impregnable against various malignant attacks as its security is based on the one-way hash function, smart card, and RSA algorithm. Performance comparison analogy that the suggested design is economical in terms of communication and computation overhead.

XiaoChun YIN et al. in 2014 used ECC based PKI [14] for certificate procedure. Because ECC vitally rebates the cost of computation, message size and transmission overhead over RSA based PKI as 160-bit key size in ECC implements equipotential security with 1024-bit key in RSA. A Secured Cloud Storage Framework (SCSF) has been devised in which the users can securely store and get data from cloud and can share data with multiple users through the unassured internet in a procure way.

Honggang Wang et al. in 2014 designed secure sharing and watermarking schemes [15] to foster users' data in the media cloud. The secure sharing scheme acquiesces users to upload multiple data pieces to different clouds, making it inaccessible to trace the whole information from any one cloud. The watermarking algorithm can be used for verifications amid personal mobile users and media cloud. Through a joint design of watermarking and Reed Solomon codes the multimedia transmission errors are refrained.

Sougata sen et al. in 2014 proposed a method of authentication which captures the behaviour [16] in which the pass code is entered. This behaviour is extracted in terms of the pressure applied on the screen by the user as well as the duration the screen is pressed. This mechanism achieves an accuracy of 84.2%.

Jeonil Kang et al.in 2014 designed a two factor face authentication scheme employing matrix transformations and user password [17]. It was designed

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

with a secure cancellation feature, in which the templates made up of permutation and feature vectors can be deliberately changed. The security enhancement methods proposed here provide security to various attacks.

Khaled M. Khan et al. in 2014 designed a model for secure transmission of matrix multiplication over cloud networking by employing randomization, column-row shuffling and alteration of matrix sizes [17]. The main aim of this model is to provide cloud users with more controls of guarding confidentiality of their data without accepting any supplementary overhead computation. By using this model, the cloud users clasp the gross secret values, without sharing with or hanging on other bodies for secret key generation, sharing and accumulation.

Faraz Fatemi Moghaddam et al. in 2013 proposed an appropriate algorithm to figure out data certainty and user authentication issues. In the framework, an encryption and key exchanging model has been interpreted based on modified Diffie-Hellman and RSA small-e [18] to split an encrypted key amid the expected recipients for transparent and risk less sharing. This client-based control system is intact, secure and righteous cloud computing accesses.

Sankardas Roy et al. in 2013 proposed a synopsis diffusion approach [19]security against attacks in which negotiated nodes add false sub aggregate values .A modernistic light weight verification algorithm figures if the computed aggregate (predicate Count or Sum) encompasses any false contribution. Regardless of the network size, the per-node communication overhead in this algorithm is o (1).

Mackay et al. in 2012 presented a concept for an innovative integrated platform [20] to reinforce the integrity and security of cloud services. This is applied in the context of critical infrastructures to identify the core requirements, components and features. The author has demonstrated how cloud computing and end-to-end networking can reasonably

be made secure enough to support critical infrastructure providers.

Qingfeng Chen et al. in 2011 proposed a formal framework [21] to deal with inconsistency in secure messages by weighting majority. The freshness and dynamics properties of secure messages are considered and a reliable function was developed to measure the belief in secure messages.

Hui li et al. in 2010 designed a compiler [22] that transforms any basic group key exchange protocol into a password authenticated group key exchange protocol. This protocol is secure in random oracle and ideal cipher models if the concealing group key exchange protocol is immune network.

Ref	Algorithm Used	Probability of Brute Force Attack	Resistant to Attack (Type)
[1]	RSA	Moderate	Impersonation attack
[2]	ECC	High	Side Channel Attack
[3]	AES	High	Man in the Middle Attack
[4]	SOTA	Low	Multi stage attacks
[5]	Asymmetric RSA	Moderate	Impersonation attack
[6]	MIP	Low	Denial of service attack
[7]	TMT and RSBS	High	Spear Phishing attacks
[8]	OSPR	Moderate	Eavesdropper attack
[9]	WEKA	Low	Drive-by attack
[10]	Random permutation	High	Denial of service
[11]	WHO-CDT	Moderate	Cross site scripting
[12]	Homomorphic Encryption	Low	Birthday attack
[13]	RSA	Moderate	Replay attack
[14]	ECC	Low	Side channel attack
[15]	Watermark Embedding	High	AI-powered attack
[16]	WEKA	Moderate	Drive-by attack
[17]	Face Authentication using vectors	High	Dictionary attack
[18]	Matrix Multiplication using Randomization	Low	Integrity attack
[19]	Modified Diffie-Hellman	High	Discrete logarithm attack
[20]	Synopsis diffusion	Moderate	Deflation attack
[21]	Critical Infrastructure	High	Insider attacks
[22]	Weighting Majority	High	Password attack
[23]	Password authenticated group key exchange compiler	High	Password attack

Fig: 4: Comparison Table for Different algorithms for Secured Online transaction.

6. CLOUD SECURITY SOLUTIONS- A Discussion

The above survey yields a result that the security in the cloud computing is highly vulnerable. It is clearly evident that password attack are just base attacks and it can be overcome by using asymmetric encryption techniques [5].The above survey yields that various algorithms have been implemented to overcome denial of service attack [10], eavesdropping attack [8], impersonation attack [5] and man in middle attack [3].The above comparison table infers that there are no stronger algorithms to withstand side channel attacks and brute force attacks. It is also seen that recent solutions were directed towards only man in middle attack, impersonation attack. Hence we need to develop stronger algorithms to withstand brute force attacks.

7. CONCLUSION

Cloud computing allows us to compose, configure and customize online; it is also flat to diversified types of attacks. This paper surveys on discrete types of attacks that

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

are possible to befall midst an online transaction. The unification of symmetric and asymmetric algorithm provides detention towards various attacks. Thus, by using Algorithms like Elliptical Curve Cryptography, Hashing – SHA256, SHA512 we can provide elevated security for online transactions.

8. REFERENCES

[1] Rajendra Patil.Harsha Dudeja,Chirag Modi "Designing an efficient security framework for detecting intrusions in virtual network of cloud computing." Science Direct-Elsevier information sciences, volume85, August 2019.

[2] Zahid Syed, Jordan Helmick, Sean Banerjee, Bojan Cukic, Touch Gesturebased Authentication on Mobile Devices: A Controlled Dataset to Study the Effects of User Posture, Device Size, Configuration, and Inter-session Variability, The Journal of Systems & Software (2018).

[3] Milad Taleby Ahvanooey, "AITSteg: An Innovative Text Steganography Technique for Hidden Transmission of Text Message via Social Media", IEEE Dataport, 2018.

[4] Joseph Gualdoni, Andrew Kurtz, Ilva Myzyri, Megan Wheeler, Syed Rizvi,Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication,Procedia Computer Science,Volume 114,2017.

[5] P. N. Hemanth, N. A. Raj and N. Yadav, "Secure message transfer using RSA algorithm and improved playfair cipher in cloud computing," *2017 2nd International Conference for Convergence in Technology (I2CT)*, Mumbai, 2017.

[6] Jolanda Modic, Ruben Trapero, Ahmed Taha, Jesus Luna, Miha Stopar, Neeraj Suri, Novel efficient techniques for real-time cloud security assessment, Computers & Security (2016).

[7] S. K. Jamagav and R. Sumathi, "Efficient and secured search on encrypted cloud data for mobile device," *2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, Bangalore, 2016.

[8] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung and L. T. Yang, "Original Symbol Phase Rotated Secure Transmission Against Powerful Massive MIMO Eavesdropper," in *IEEE Access*, vol. , 2016.

[9] A. Salem, D. Zaidan, A. Swidan and R. Saifan, "Analysis of Strong Password Using Keystroke Dynamics Authentication in Touch Screen Devices," *2016 Cyber security and Cyber forensics Conference (CCC)*, Amman, 2016.

[10] P. Daffu and A. Kaur, "Low cost robust inter-server authentication for cloud environments," *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, 2016.

[11] R. Pragaladan and S. Sathappan, "High Confidential Data storage using DNA structure for cloud environment," *2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)*, Bangalore, 2016.

[12] K. K. Chauhan, A. K. S. Sanger and A. Verma, "Homomorphic Encryption for Data Security in Cloud Computing," *2015 International Conference on Information Technology (ICIT)*, Bhubaneswar, 2015.

[13] Preeti Chandrakar, Hari Om,"RSA Based Two-factor Remote User Authentication Scheme with User Anonymity",Procedia Computer Science, Volume 70,2015.

[14] X. C. Yin, Z. G. Liu and H. J. Lee, "An efficient and secured data storage scheme in cloud computing using ECC-based PKI," *16th International Conference on Advanced Communication Technology*, Pyeongchang, 2014.

[15] H. Wang, S. Wu, M. Chen and W. Wang, "Security protection between users and the mobile media cloud," in *IEEE Communications Magazine*, vol. 52, March 2014.

[16] Sen, Sougata & Muralidharan, Kartik. (2014). Putting â€˜pressureâ€™ on mobile authentication. 2014 7th International Conference on Mobile Computing and Ubiquitous Networking, ICMU 2014.

[17] Kang, Jeonil & Nyang, Daehun & Lee, KyungHee. (2014). Two-factor face authentication using matrix permutation transformation and a user password. Information Sciences.

[18] K. M. Khan and M. Shaheen, "Empowering users of cloud computing on data confidentiality," *2014 IEEE 3rd International Conference on Cloud Networking (CloudNet)*, Luxembourg, 2014.

[19] S. Ben Othman, A. Trad, H. Youssef and H. Alzaid, "Secure data aggregation in wireless sensor networks," *2013 12th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET)*, Ajaccio, 2013.

[20] Fatemi Moghaddam, Faraz & Varnosfaderani, Shirin & Ghavam, Iman & Mobedi, Soroush" A Client-Based User Authentication and Encryption Algorithm for Secure Accessing to Cloud Servers".IEEE Student Conference on Research and Development in 2013.

[21] Mackay, Michael & Baker, Thar & Al-Yasiri, Adil. "Security-oriented cloud computing platform for critical infrastructures" in 2012.

[22] Chen, Qingfeng & Zhang, Shichao "Dealing with Inconsistent Secure Messages"in 2011.

[23] Li, Hui & Wu, Chuankun & Sun, Jun A general compiler for password-authenticated group key exchange protocol in 2010.

[24] Mahavir Jain, and Arpit Agrawal, "Implementation of Hybrid Cryptography Algorithm", International journal of Core Engineering & Management, Volume 1, Issue 3, pp. 1-8, June 2014.

[25] F. Sardis et al., "On the Investigation of Cloud-Based Mobile Media Environments with Service-Populating and QoS-Aware Mechanisms," IEEE Trans. Multimedia,vol. 15, no. 4, June 2013, pp. 769–77.