Security Enhancement and PaaS platform Authentication in Cloud Computing based On SBA

Ramdas Vankdothu (vramdas786sap@gmail.com)
Osmania University University College of Engineering https://orcid.org/0000-0002-8478-1291
Mohd Abdul Hameed
Osmania University

Research Article

Keywords: PaaS platform authentication, security enhancement, cloud computing, Signature Based Authentication, Public-key value-based signature generation, Public-key value-based signature verification

Posted Date: November 9th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-993027/v1

Security Enhancement and PaaS platform Authentication in Cloud Computing based On SBA

A.Ramdas Vankdothu, B.Mohd Abdul Hameed

Abstract—One of the most challenging security requirements in a PaaS platform setting is authentication. We provide a new signature-based authenticated key establishment approach for PaaS platform security improvement in this study. It adds a feature to increase confidentiality and non-repudiation by requiring the sender to sign a specific action while sending data from one user to another. It's signed with the transaction's private key and a public-key value-based signature generated with the transaction's public key. Use the public key value-based signature that was generated to authenticate this operation, and the hashing process assures that the operation is immutable. Our proposed solution delivers improved data security, throughput, reaction speed, and a reduction in end-to-end delay and overhead when compared to existing methodologies. The results of the experiments reveal that the proposed system achieves a superior outcome to the existing methods. This project makes use of the MATLAB platform.

Index Terms—PaaS platform authentication, security enhancement, cloud computing, Signature Based Authentication, Public-key value-based signature generation, Public-key value-based signature verification.

1. INTRODUCTION

The latest progress of distributed computing has shown its capacity to change the advancing method. A striking IT gear is envisioned and gotten [1]. In dispersed processing, the enlisting organizations can be requested into Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) [2]. Limit as-an organization has ascended as a business elective for close by data accumulating due to its characteristics consolidate less starting establishment course of action, easing from upkeep overhead and total entry to the data autonomous of zone and contraption [3]. Cloud storing, which is one of the various cloud organizations, fills in as a rational mechanical assembly and has made data redistributing to the cloud a creating design [4]. Circulated stockpiling is a favorable fundamental position of conveyed processing. It has been coherently essential since it can give insignificant effort and on-demand utilize fitting to extensive limit and dealing with resources [5]. Starting late, dispersed registering has ascended as another stage for passing on, directing, and giving gigantic extension data organizations through an Internet-based system. Productive models consolidate Amazon EC2, Google App Engine, and Microsoft Azure. By re-appropriating data and organizations, cloud customers welcome an adaptable phenomenal help with a money related and beneficial path since they can capably manufacture their additional room as and when required without buying any limited devices [6].

A. Ramdas Vankdothu is pursuing his Doctoral degree in Computer Science & Engineering at Osmania University Hyderabad, India (e-mail: vramdas786sap@gmail.com).

B. Mohd Abdul Hameed, Assistant Professor in Department of Computer Science & Engineering University College of Engineering (A). Osmania University Hyderabad, India.

They are as follows: (1) users can access the indirectly set aside data at any time and from any location, and endorsing customers can share the data. (2) Customers can be mitigated from the heaviness of the board at a local level, (3) Capital usage on gear and programming costs can be avoided, and so on [7]. Customers can use complete game plans of instruments for assessing various applications, accumulating and arranging through the Internet, similar to using the organizations offered by cloud creators [8], when access is powered by dispersed processing.

There are two standard attacks for data set aside in the cloud under such conditions, i.e., external attacks began by unapproved outcasts, and internal attacks began by scheming CSPs. Now and then, we can't totally trust in a CSP, yet simultaneously need its organizations. , it is basic to give sufficient well-being to protect the set aside data both from noxious distant attacks and the pro association itself. This nonattendance of trust is essential as it brings new security issues towards the cloud condition [9]. Therefore, a couple of frameworks are relied upon to guarantee the customer data security and the customer addressing insurance in a cloud space [10]. Hence data owners demand raised degrees of security and arrangement when they re-proper their data to a cloud; disregarding the way that they generally speaking scramble their data while taking care of it in a cloud specialist, they notwithstanding all that need control over it, for example, if they a great part of the time update it. Direct work of traditional cryptographic locals can't achieve the data security required [11]. Disregarding the specific and financial positive conditions of disseminated registering, various potential cloud purchasers are up 'til now hesitant to get dispersed processing due to security and insurance concerns. These security and assurance concerns exist due to the way that, by far, most of the security controls and

measures by cloud specialist organizations (CSPs) are not clear to the cloud administration clients (CSUs) [12]. During the time differing encoding approaches have been made and used feasibly to protect such sensitive datasets. Regardless, these strategies wound up being irrational, exorbitant and inefficient. Truly, the confirmation of the cloud datasets by methods for encryption is extraordinarily inconvenient and testing, considering that most current applications rely upon decoded datasets [13].

These days there are many moved encryption strategies for enormous data security sparing plans and are recorded as follows, Attribute-based encryption (ABE) is envisioned as an outstandingly reassuring open key rough for recognizing versatile and fine-grained get the opportunity to control structures, where differential yet versatile access rights can be distributed to particular customers. Especially, figure text-strategy trait based encryption (CP-ABE) engages data owners to show a passage technique over a tremendous region of attributes and encode the data under the passageway methodology with the relating open key sections. Interpreting is enabled if the customer's characteristics facilitate the relating access technique [14]. By then in the conveyed registering and gigantic data circumstances, Order-safeguarding encryption (OPE) will be more important, considering the way that redistributed data set has pulled in much thought starting late on account of the ascent of disseminated processing, in any case, how to guarantee the re-appropriated data taking care of in the untrusted cloud specialist transforms into a troublesome issue. Since demand protecting, OPE grants untrusted laborers to perform information base undertakings, such as connection and range question over encoded data, without unscrambling them [15]. Despite the pushed procedures made, it is attempting to design and recognize solid assurance defending systems. This test begins from the battling fundamental catalysts that system modelers need to at the same time consider [16]. Likewise, applying these standard approaches to manage colossal data anonymization presents versatility and adequacy challenges because of the "3Vs", i.e., Volume, Velocity and Variety [17]. In particular, it is so far a test to successfully achieve security protection over appropriated, and consistent data inside seeing data invigorates [18].

1.1. Contribution and organization of the paper:

The fundamental contribution of this suggested approach is a new signature-based verified key establishment scheme that improves PaaS platform security. Our study outlines a novel authentication system that includes the phases of public key value based signature generation, encryption, signature verification, and decryption. The procedures are outlined in detail in the parts that follow;

The rest of the paper is organized as follows; Section 2 presents the review of related works. Section 3 presents the problem statement and the proposed signature-based authenticated key establishment scheme for PaaS platform security enhancement model explained in section 4. The experimental results are analyzed in section 5 and conclusion part is presented in section 6.

2. LITERATURE SURVEY

Yong Yu et al. [19] have demonstrated a significant advancement in character-based (I-D) Remote data integrity checking (RDIC) by utilizing key-homomorphic cryptographic essentials to reduce system complexity and the total for presenting and dealing with the open key accolade structure in public key infrastructure (PKI) based RDIC plans. It includes security touching a burning cloud specialist and a zero accomplishments puzzle going up against an outcast verifier and formalizing ID-based RDIC and its security architecture. During the RDIC technique, the suggested ID-based RDIC display provides no information about the saved data to the verifier. The new invention is secure against the harmful specialist in the standard social event model and obtains zero data puzzle near a verifier. The results of a broad security review and approval have been identified.

Xuefeng Liu et al. [20] has demonstrated innovative message-bolted trustworthiness examining plan applicable to both record level and knock level duplicating systems without using an extra arbiter laborer. This arrangement is limitable in the same way that invalidating the code text superfluousness is. It uses a message-decided stamping key to enable reliability name deduplication, which only acknowledges non-essential client-side calculating overhead. By combining the mediator re-signature approach, thoroughly complete the uprightness examination over any client's circulated stockpile. The creative arrangement will not betray data ownership information in the optional prophet model and is probably safe under the Computational Diffie-Hellman (CDH) question. The execution examination has finally been defined.

Yue Zhang et al. [21] established an unmistakable stockpile reviewing plan that sanctions substantially profitable customer denial free of the full scale number of record squares compelled by the disavowed customer in the cloud. This is fostered by developing a novel key age calculation approach and a new private key update mechanism. Using this structure and method, we can detect client denial by resurrecting the non-disavowed complete customers' private keys instead of the rejected customer's authenticators. When the authenticators are not restored, the dependability investigation of the repudiated client's information is currently sufficient. Meanwhile, the demonstrated system is based on character-based cryptography, which eliminates the tangled affirmation

association that is evaluated in normal Public Key Infrastructure (PKI) structures.

Raman Kumar et al. [22] made three-level security engineering to take care of sight and sound records that join work base access control, encryption, and imprint check. As a result, a more secure dynamic analysis show is advised, one that can precisely store data in the cloud. Here, the combiner and the third-party auditor (TPA) may vouch for the consistency of the quality based on the information they get from one another. As a result, the developed secure dynamic assessing display is safe and useful against a variety of conspiracies.

Yang et al. [23] passed on a proficient public inspecting arrangement that could spare the character security and the character perceptibility for pack people simultaneously. Specifically, the first arranged another structure for data participating in the cloud and formalized the significance of the open assessing plan for shared cloud data supporting character insurance and perceptibility. Also, they grew such an arrangement in which a social affair head was familiar with help part's made authenticators to guarantee the character security and two records were used to record the people who played out the latest change on each square to achieve the character perceptibility.

3. PROBLEM STATEMENT

- In the past decade, Work focused on the attack-oriented but focused on authentication cloud server data in this work.
- Eavesdrop attack with the help of past search history, sometimes it's possible for the hacker to access the details from the cloud server.

4. PROPOSED METHODOLOGY

An efficient signature-based authentication is used; a signature-based authentication generator computes a real-time signature on the suspect object. In previous work, the user accessed data's are pre-processed based on that OCSA optimally selects the feature data's, and these all data's are move to the next stage of attack detection. RNN classifies attacked data and normal data. Finally, attacked data are removed. Only the normal data are move to the next phase of security enhancement. The concept includes the combinations of oppositional crow search algorithms as well as recurrent neural network (RNN). Further improve its security, in this paper we propose an efficient novel signature based authentication for secure an encrypted data. In comparison to standard digital signature schemes, the novel technique simultaneously achieves authenticity, data integrity, anonymity, and accountability. Finally, we present a probabilistic signature verification system that can detect tempered or unauthorised messages.

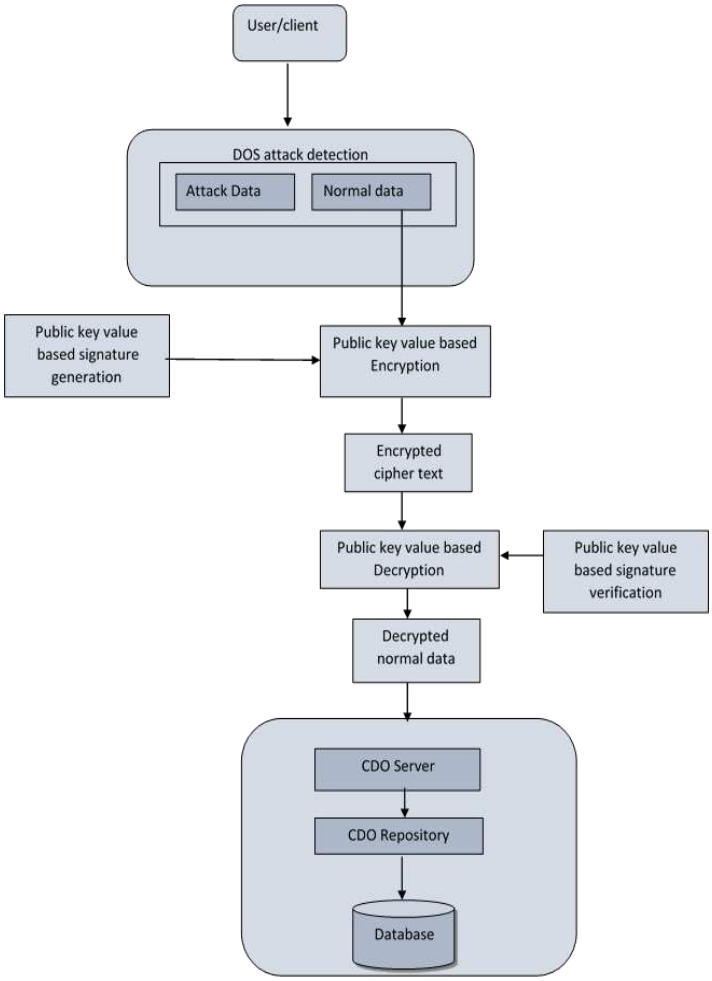

Figure 1: Overall system architecture

As shown in figure 1, the user accessed data are pre-processed based on that OCSA optimally selects the feature data's, and these all data's are move to the next stage of attack detection. RNN classifies attacked data and standard data. Finally, attacked data are removed. Only the normal data's are move to the next phase of security enhancement. Further improve its security, our paper proposes signature based authentication is used for secure an encrypted data. At first, a public key value based signature is generated for all the user data's based on the signature generation the user data's are encrypted. Then the encrypted data are verified based on a public key value based signature. Afterward, data signature is verifies and decode. The whole concepts are explained in detail as followings section;

4.1. PaaS platform authentication and security enhancement:

Signature based authentication:

In this, an effective, adaptable and secure plan for group signature based validation is proposed. Our plan gives the adaptable answer for the verification and security of the PaaS stage. Signature is utilized to check the data between both the sender and receiver side. The calculation utilized for the signature generation is given in calculation 1.

Step1: signature generation algorithm takings as input public key based arbitrary statistics $(g1, g2)$

Step2: G is primarynumeralas well as a message M , and profits as follows.

Step3: Hand-pickedarbitrary number α, β

Step4: Calculateassistant values

$T1 = g1 \oplus \alpha, T2 = g2 \oplus \beta$

Step5: Calculatepublic key value

Step6: Calculate a test value C by means of

$C \leftarrow H(M, E_y, T1, T2)$

Step7: Output the signature $\sigma \leftarrow (\alpha, \beta, C, T1, T2)$.

Algorithm 1: Encryption using Public key value based signature generation

In algorithm 1, signature generation for the PaaS platform security is improved by the key values. Key value is sum of every data makes a random variable for which expected esteem or average is the key value which is evaluated for the informational collections by utilizing condition (7),

$$E_y = \sum_{i=1}^{2} P(T_i) \log_2 \{P(T_i)\} \qquad (7)$$

Where, $P(T_i)$ is the probability of selected of i^{th} feature. After the, Public key value based signature generation all the user accessed data are encrypted. The concepts are explain detailed as following sections;

Example of file signature and encode by X:

♦ X needtowardshandover its file to Y

♦ Produceindividuality $X(ID_x, N_x)$ as well as $Y(ID_y, N_y)$

♦ At that time,calculate hash value the $PW_x = h(N_x \| N_y)$

♦ T1 is provision value which is intended by $T1 = ID_x \oplus N_B$

♦ Public key value based signature generated $SX_x = h(T1 \| PW_x) \oplus ID_B$

♦ Private key based encrypting $EF = ENC(F, PK)$

♦ lastlyenhance the public key based signature in the encrypted file by means of

$SX_{Enc} = E_{UAD}(ID_Y, N_Y, SX_X, T1, EF)$

4.2. Public key value based signature verification:

In the Public key value based signature verification measure, the public key is utilized to confirm the signature to get the data access. The calculation utilized for the public key value based signature verification process is appeared in calculation 2.

Step1: Re-derive $\acute{T}_1$, $\acute{T}_2$

Step2: Calculate assistant values $\acute{T}_1 = T_1 \oplus \alpha$, $\acute{T}_2 = T_2 \oplus \beta$

Step3: Calculate publickey values

Step4: Calculate a task Ĉ ←H(M, E_y , Ť1, Ť1)

Step5: Chequered that the task [C = = Ĉ]

Step6: If it is agree to take then and there signature is verified. Or elsereject.

Algorithm 2: Encryption using Public key value based signature generation&verification

On the off chance that the test esteem is equivalent in coordinating, the confirmation step results in the signature as a substantial one. Furthermore, the information is imparted to the mark checked client. On the off chance that the test esteem isn't equivalent, at that point the client results the signature as invalid one and furthermore the information isn't imparted to that client. This public key worth based mark confirmation measure doesn't permit any aggressors to drop the client got to information just as doesn't permit including any undesirable data with the first information. Appropriately, the attack is kept away from by utilizing our proposed signature based authentication measure.

Example of file signature verifies and decode by Y:

♦ Afterwardin receipt of the message, Y initially decrypts $S_{UAD} = D(SY_{UAD})$ to disclose $S_{UAD}, SDN_{En}, T2$

♦at that time calculate $T2 = T1 \oplus N_y \; and \; SX_x = h(T2 \| PW_x) \oplus ID_y)$, then SX_x chequered whether $SY_y = SY_{FX}$ if they are equal, file is decipheror else not

♦ The file is decoded by means of private key $S = D(SDN_{Enc})$

4.3. Encoding and Decoding Algorithms:

Input: X: Source, Y: Destination F: Message

Output: SX_{Enc} : Encode File

Begin

Parameters:

ID_x, N_x :Identity of source||IP address of source

ID_y, N_y : Identity of destination||IP address of destination

ID_{UAD}, N_{UAD} : Authentication as well as security augmentation

PK1, PK2: Key||public also private key

T1: Provision value

SX_x : Signature

H: Hash function

Function: Calculate hash value

If $N_X \neq N_Y$ do

$PW_X \leftarrow h(N_X \parallel N_Y)$

$T_1 \leftarrow ID_X \oplus N_Y$

$SX_x \leftarrow h(T1 \parallel PW_X) \oplus ID_Y$

Else

Reappearance error message

End

Function: Encryptingas well as signature generation

While $F \neq EOF$ do

$F \leftarrow Enc(F, PK1)$

$SX_{Enc} \leftarrow E_{UAD}(ID_Y, N_Y, SX_X, T1, F)$

End

Function: Authentication

$T2 \leftarrow ID_{UAD} \oplus N_X$

$UAD_{Enc} \leftarrow SX_{Enc}$

$SY_{UAD} \leftarrow E(T2, UAD_{Enc}, N_Y)$

End

Algorithm 3: Encoding

Calculation 3 is a depiction of the Public key value based signature based information Encoding as well as Signature generation. The cycle arrangement for proposed PaaS platform authentication as well as security upgrade as follows:

Step1: Calculate the hash value

- Initiallychequered the individuality of the source as well as destination $N_x \neq N_Y$ if there is equivalentlay off the mixtureor elsecalculate the values $PW_Y, T1, SX_x$

Step2: Encryptingas well as signature generation

- Chequered the condition, if it is true to do encoding in addition to signature generation process.
- Source X produce the data as well as send towards the destination Y Source X encrypts the analysis data F into cryptograms by means of the private key PK1.
- cryptograms the analysis data from the ring signature asSAEnc. It can be occupied as a pattern to check the same data reserved twice in storage. The SAEnc sends the series of data towards the network.

Input: SY_{UAD} : Encode File

Output: S: Decode File

Begin

Parameters:

D: decoding

SC: Authenticated certificate

SR_X : Signature

Function: XOR

IF $SY_{UAD} \neq EOF$ then

$SY_{UAD} \leftarrow XOR(SY_{UAD})$

$SY_{UAD}\ get(UAD_{En}, T2, N_Y)$

End

Function: verify signature as well as decode

$T3 = T2 \oplus N_Y$

If $T_2 == T_3$ then

UAD is authenticated

$U \leftarrow A(UAD_{Enc}) \parallel publickey$

$SR_X = h(T2 \parallel PW_X) \oplus ID_Y$

Get the S from S_{Xx}

If $SR_X == SX_X$ then

X is authenticated.

$SC_Y = h(T2 \parallel ID_Y \parallel ID_{UAD} \parallel N_{UAD})$

$SC = E_Y(C_Y, cert)$

End

End

End

Algorithm 4: Signature verifies and decode

These steps demonstrate that the proposed technique finds the secure authentication to ensure attacks and achieves significant execution gain.

5. RESULTS & DISCUSSION

The proposed signature based authenticated key foundation conspire for PaaS platform security improvement. In this segment, the proposed strategy is actualized in MATLAB on a framework having 6 GB RAM and 2.6 GHz Intel I-7 processor. For deciding the precision, transfer speed, inactivity, reaction time, throughput and season of the strategy are estimated and examined and the client got to information are gathered from the dataset.

5.1. Evaluation Metrics:

The success of the suggested technique is determined by calculating specific presentation metrics.

Accuracy: The proportions of affectability and explicitness define accuracy. This is what it means:,

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100 \quad (8)$$

Throughput: It is the quantity of information that can be sent from the sources to the objective every second. Unit of this boundary is Mbps.

$$Throughput = \frac{Amount\ of\ transmitted\ data\ (Mb)}{Transmitted\ time\ (s)} \quad (9)$$

Overhead: Number of additional bytes added to the data packet to communicate the information.

5.2. Comparative Analysis:

The performance of a proposed signature-based authenticated key establishment scheme for PaaS platform security enhancement is analysed with the help of accuracy, bandwidth, latency, response time, throughput as well as time which are most significant performance parameters. Our proposed method is compared to SVM, MSVM, CAMEL, and ECCTS, which are all well-known decision trees. The enhancement of an authentication and security phase is verified in the result area. Figure 2-7 depicts the approach's effectiveness.`

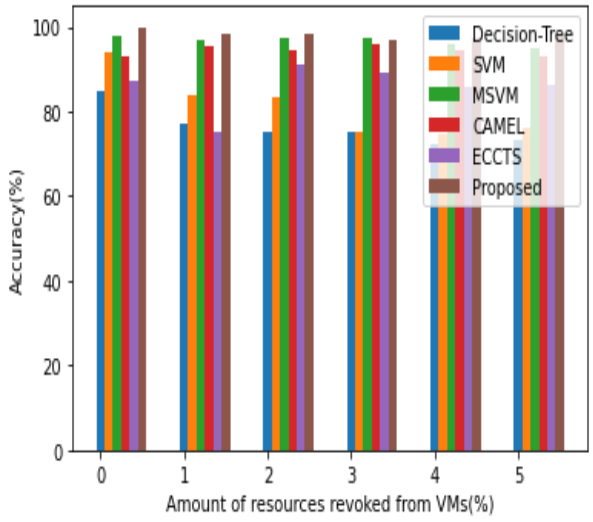

Figure 2: Performance analysis of Accuracy

The accuracy of a new method is compared to that of existing decision trees, SVM, MSVM, CAMEL, and ECCTS in the graph2 above. When analysing figure 2, the highest level of accuracy is obtained. Our proposed strategy outperforms other existing solutions in terms of results.

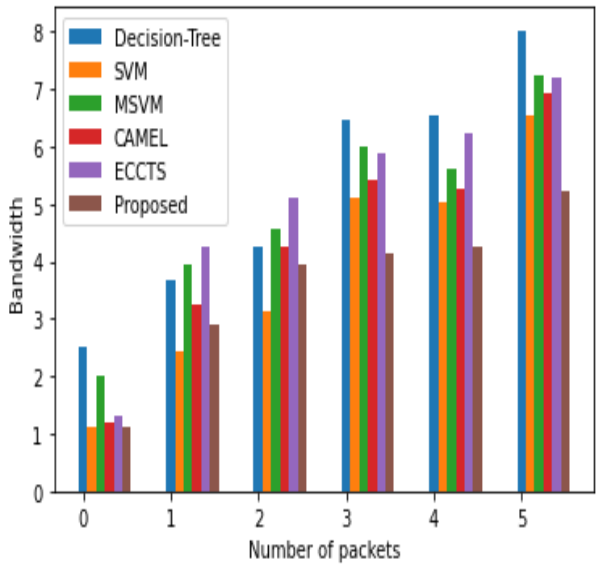

Figure 3: Performance analysis of Bandwidth

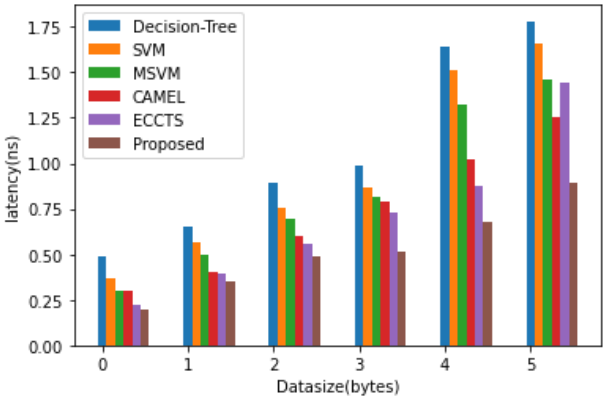

Figure 4: Performance analysis of Latency

The bandwidth and latency in the file transmission are measured and plotted in Figs. 3 and 4, respectively, after integrating the proposed authentication technique.The above figure shows the performance of bandwidth and latency which is compared with the existing decision tree, SVM, MSVM, CAMEL and ECCTS. When analysing figure 2 proposed obtains the highest outcome of bandwidth as well as latency.

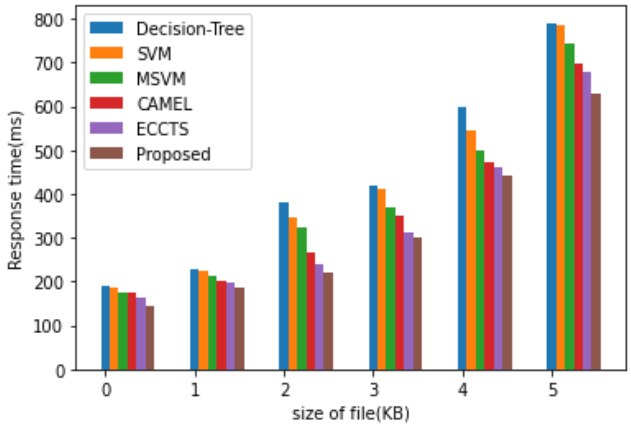

Figure 5: Performance analysis of Response time (ms)

Figure 5 depicts network parameters such as data transfer reaction time. Figure 5 shows that our proposed approach achieves a better result than other existing decision tree, SVM, MSVM, CAMEL, and ECCTS techniques.

Figure 6: Performance analysis of Throughput(Mbps)

Users in the network request transactions among themselves. The throughput time of a network is the number of such transactions. Figure 6 compares the throughput of this procedure to that of previous approaches. Several transaction requests are recorded in this verification, and it yields a superior result.

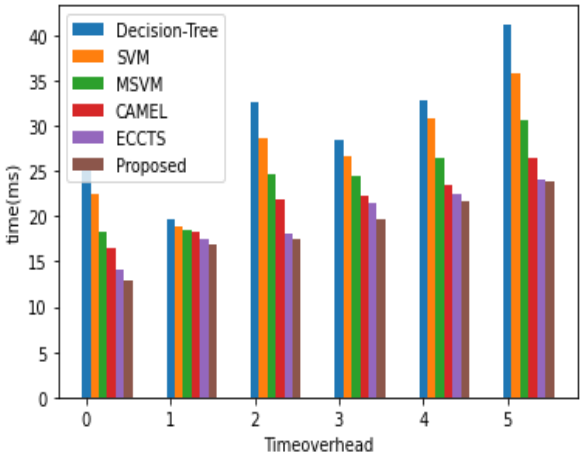

Figure 7: Performance analysis of Time overhead (ms)

Figure 7 displays the time overhead compared with the existing method. The findings show that there isn't much of a difference in time overhead; even a millisecond difference can be detected.The above figure shows the performance of time overhead which is compared with the existing decision tree, SVM, MSVM, CAMEL and ECCTS. When analysing figure 7 proposed obtains the highest outcome.

6. CONCLUSION

Today, we face extraordinary difficulties as far as protecting protection, information security and trustworthiness with the ever-expanding use of a few cloud stages and interest for shrewd administrations. Tending to these issues ought to be the quick need of the scientists. To address this issue, we introduced another authentication technique to PaaS platform authentication and security upgrade in cloud computing dependent on SBA. Public key value based signature is created for all the user data's based on the signature generation the user data's are encrypted. The encrypted data is then confirmed using a signature based on a public key value. After then, data signature verifies and decodes the information.The experimental results are explained our approach achieves the maximum accuracy, bandwidth, latency, response time, throughput as well as time compared to existing decision tree, SVM, MSVM, CAMEL and ECCTS approaches.We can see from the conversation that our proposed strategy is superior to the current outcomes.

Reference:

[1] Wei, Lifei, Haojin Zhu, Zhenfu Cao, Xiaolei Dong, Weiwei Jia, Yunlu Chen, and Athanasios V. Vasilakos. "Security and privacy for storage and computation in cloud computing." Information Sciences 258 (2014): 371-386.

[2] Wang, Boyang, Baochun Li, and Hui Li. "Panda: Public auditing for shared data with efficient user revocation in the cloud." IEEE Transactions on services computing 8, no. 1 (2015): 92-106.

[3] Liu, Chang, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang, and Jinjun Chen. "MuR-DPA: Top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud." IEEE Transactions on Computers 64, no. 9 (2015): 2609-2622.

[4] Kumar, Raman, and Gurpreet Singh. "Analysis and design of an optimized secure auditing protocol for storing data dynamically in cloud computing." Materials Today: Proceedings 5, no. 1 (2018): 1037-1047.

[5] Ni, Jianbing, Yong Yu, Yi Mu, and Qi Xia. "On the security of an efficient dynamic auditing protocol in cloud storage." IEEE Transactions on Parallel and Distributed Systems 25, no. 10 (2014): 2760-2761.

[6] Song, Wei, Bing Wang, Qian Wang, Zhiyong Peng, Wenjing Lou and Yihui Cui, "A privacy-preserved full-text retrieval algorithm over encrypted data for cloud storage applications", Elsevier on Journal of Parallel and Distributed Computing, pp.1-25, 2016.

[7] Pasupuleti, Syam Kumar, Subramanian Ramalingam and RajkumarBuyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing", Elsevier on Journal of Network and Computer Applications, Vol.64, pp.12-22, 2016.

[8]AqeelSahi, David Lai and Yan Li, "Security and privacy preserving approaches in the Health clouds with disaster recovery plan", Elsevier Journal of Computers in Biology and Medicine, Vol.78, pp.1-8, 2016.

[9] Worku, Solomon Guadie, Chunxiang Xu, Jining Zhao and Xiaohu He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage", Elsevier on Computers & Electrical Engineering, Vol.40, No.5, pp.1703-1713, 2014.

[10] Liu, Qin, Guojun Wang and Jie Wu, "Secure and privacy preserving keyword searching for cloud storage services", Elsevier on Journal of network and computer applications, Vol.35, No.3, pp.927-933, 2012.

[11] Dong, Xin, Jiadi Yu, Yuan Luo, Yingying Chen, GuangtaoXue and Minglu Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing", Elsevier on computers & security, Vol.42, pp.151-164, 2014.

[12] Razaque, Abdul and Syed S. Rizvi, "Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment", Computers & Security, Vol.62, pp.328-347, 2016.

[13] Aldeen, Yousra Abdul Alsahib S., MazleenaSalleh and YazanAljeroudi, "An innovative privacy preserving technique for incremental datasets on cloud computing", Elsevier on Journal of Biomedical Informatics, Vol.62, pp.107-116, 2016.

[14] Zhang, Yinghui, Xiaofeng Chen, Jin Li, Duncan S. Wong, Hui Li and Ilsun You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing", Elsevier on Information Sciences, pp.1-20, 2016.

[15] Liu, Zheli, Xiaofeng Chen, Jun Yang, Chunfu Jia and Ilsun You, "New order preserving encryption model for outsourced databases in cloud environments", Elsevier on Journal of Network and Computer Applications, Vol.59, pp.198-207, 2016.

[16] Mortaza S. Bargh, Sunil Choenni and Ronald Meijer, "On design and deployment of two privacy-preserving procedures for judicial-data dissemination", Elsevier on Government Information Quarterly, pp.1-13, 2016.

[17] Vennila.S and J. Priyadarshini, "Scalable Privacy Preservation in Big Data a Survey", Elsevier on Procedia Computer Science, Vol.50, pp.369-373, 2015.

[18] Zhang, Xuyun, Chang Liu, Surya Nepal and Jinjun Chen, "An efficient quasi-identifier index based approach for privacy preservation over incremental data sets on cloud", Elsevier on Journal of Computer and System Sciences, Vol.79, No.5, pp.542-555, 2013.

[19] Yu, Yong, Man Ho Au, Giuseppe Ateniese, Xinyi Huang, Willy Susilo, Yuanshun Dai, and Geyong Min. "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage." IEEE Transactions on Information Forensics and Security 12, no. 4 (2017): 767-778.

[20] Liu, Xuefeng, Wenhai Sun, Wenjing Lou, Qingqi Pei, and Yuqing Zhang. "One-tag checker: Message-locked integrity auditing on encrypted cloud deduplication storage." In INFOCOM 2017-IEEE Conference on Computer Communications, IEEE, pp. 1-9. IEEE, 2017.

[21] Zhang, Yue, Jia Yu, RongHao, Cong Wang, and Kui Ren. "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data." IEEE Transactions on Dependable and Secure Computing (2018).

[22] Kumar, Raman, and Gurpreet Singh. "Analysis and design of an optimized secure auditing protocol for storing data dynamically in cloud computing." Materials Today: Proceedings 5, no. 1 (2018): 1037-1047.

[23] Yang, Guangyang, Jia Yu, Wenting Shen, Qianqian Su, Zhangjie Fu and RongHao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability", Journal of Systems and Software, Vol.113, pp.130-139, 2016.