IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received August 10, 2020, accepted August 23, 2020, date of publication September 9, 2020, date of current version September 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3022957

Enhancing the Access Privacy of IDaaS System Using SAML Protocol in Fog Computing

CH. RUPA[1], (Senior Member, IEEE), RIZWAN PATAN[1], FADI AL-TURJMAN[2], (Member, IEEE), AND LEONARDO MOSTARDA[3], (Member, IEEE)

[1]Department of Computer Science and Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada 520007, India
[2]Research Center for AI and IoT, Artificial Intelligence Engineering Department, Near East University, 99138 Nicosia, Turkey
[3]Computer Science Division, University of Camerino, 62032 Camerino, Italy

Corresponding author: Rizwan Patan (prizwan5@gmail.com)

ABSTRACT Fog environment adoption rate is increasing day by day in the industry. Unauthorized accessing of data occurs due to the preservation of Identity and information of the users either at the endpoints or at the middleware. This paper proposes a methodology to protect and preserve the Identity during data transmission of the users. It uses fog computing for storage against security issues in the cloud and database environment. Cloud and database architectures failed to protect the data and Identity of users but the Fog computing based Identity management as a service (IDaaS) system can handle it with Security Assertion Mark-up Language (SAML) protocol and Pentatope based Elliptic Curve Crypto cipher. A detailed comparative study of the proposed and existing techniques is investigated by considering multi-authentication dialogue, security services, service providers, Identity, and access management.

INDEX TERMS Fog computing, IDaaS, integrity, SAML, Pentatope-based ECC, authentication dialogues.

I. INTRODUCTION

Now a day, one of the essential services which can allow into the cloud-based organizations is Identity management as a service (IDaaS) [1]. It causes to enrich and deploy security services like accountability, authorization, and access control in the cloud environments [1]. Even though, Cloud paradigm environment plays a vital role in the computing field regards to monitor and control the data. IDaaS facilitates Infrastructure to Identity management as well as permits to turn towards the on-demand delivery model as modern techniques from a traditional approach to promise delivery model. Moreover, IDaaS offers various opportunities for cloud users and providers such as cost reduction, controlling on outsourced data, which is related to the user's identity [2]. It extends to that broadening its service offers in the direction of facilitating the security services.

Globally, advanced technologies like Fog and edge computing infrastructure [32]and blockchain technology [38] utilization rate increased due to maintains the vast amount of data that is collected from the IoT connecting devices. This Infrastructure has attracted by the users of a large number of connected automated devices. However, these computing systems use to analyze the storing data at cloud/fog concerning its characteristics like storage, computation, and analysis (SCA). In this proposed work a prototype developed and demonstrates how can IDaaS systems protect the privacy of a user's data. This prototype has designed and developed using Security Assertion Mark-up Language (SAML) identity management protocol [3], and a Pentatope based ECC (PECC) scheme [7] for executing the cryptographic preservation in cloud-based applications. This technique will enable an ID facilitator to provide required attributes to the service requestor without extract and read the values. In this way user's privacy preserves in respect of ID provider. An identity provider to serve attributes to other parties without being able to read their values, preserving in this way users' privacy concerning the identity provider [4]. A comparative analysis will be made concerning its performance using various Identity Management Protocols.

SAML is a standardized and secured with an excellent user experience. And uses as a SPOA means that single point of authentication [3]. At a secure ID (Identity) provider SAML based proposed system verifies the credentials of the user.

The associate editor coordinating the review of this manuscript and approving it for publication was Gautam Srivastava.

And monitor and check whether the user credentials crossing over the firewall boundary or not. It shows that not required to preserve or synchronize the IDs in any proposed cloud-based applications. It may cause to steals the data from the breaches of the storages [5]. PKI (public key Infrastructure) based SAML make available a strong security layer to protect the IDs over the security attacks [18]. Public Key Infrastructure (PKI) based PECC is used for extra security purpose like two level security.

The proposed work protocol helps to enhance privacy to the data of users/enterprise using Pentatope based ECC cipher (PECC) [7]. Related work or literature survey of the proposed work has mentioned in section 2. In Section 3 discussed the work which can used to improve the process of secure integrity checking of Identity of the cloud users through IDaaS (Identity as a Service) and PECC. Amazon EC2/Google App Engine Cloud Environment/ Set up used to implement the protocol and tested and analysed the attack possibilities as discussed in section 4.

II. LITERATURE SURVEY

Privacy and protection with authentication feature became a part in every communication system. Different identity management systems and protocols were offering the privacy and protection-based services with efficient management of identities and the keys. The initial steps to achieve privacy and protection are trust development among the entities.

Jing *et al.* [1] has proposed an authentication model using SAML protocol in the cloud environment. In this author analysed the security issues in bidirectional authentication process and to overcome this problem, a link is added using the certificate authority and the challenge response generated by the identity provider. It distributes the session key to the users and the service providers. It provides some methods that guarantees the session essential security, such that it solves some problems related to the information transmission. By the uniform identity resource management one can resist the occurrence of replay attacks in the resource transformation.

Indu *et al.* [2] has developed a model to provide to provide a secure identity and access management (IAM) system in the cloud environment. It was achieved by developing IAM with several authentication and authorization protocols. It depicts the validation of user identities and hiding of original identities of the user. It can be done by providing various security protocols in the cloud identity management system.

Wang *et al.* [3] proposed a mechanism which provides security to the identities as well as for the applications and access resources based on cloud environment. In the manual identity management system, there is a possibility that the third-party vendors may misuse the user credentials for malicious attacks in the cloud. So, a single-sign-on mechanism is introduced, which helps the user's one-time password to access applications and access resources every time. It depicted how the authentication is provided using OpenID, OAuth and SAML protocols [4]. No password sharing to the associated applications present in the cloud can be achieved by using these authentication protocols. Some authorization mechanisms are also introduced in this, which helps to permit or deny the access to cloud users for a particular resource. There by the process is purely transparent to the entities wishing to communicate each other for a specific service. This is helpful to reduce the incarnation of the identity theft attacks in the cloud environment.

Jiang *et.al* [5] analysed and spotted several security issues, identity threats and limitations in the cloud environment with prominence on identity and access management, security services. This study compares various protocols with their frequently used mechanisms with different perspectives.

From the existing literature we can notice that these protocols are used only to hide the identities of the end users communicating through the cloud but not for the information that is transmitted over the cloud by considering various parameters like Infrastructure as a service (IaaS) [6], [14].

The existed methods unable to focus on authentication validity [16], [20], [21] during the data flow over the cloud environment. To provide security for the identities and the information and the flow of data, proposed framework makes use of the SAML protocol, strong authentication sever and IDS servers for authentication purpose and Pentatope based Elliptic Curve Cryptography [7] to transfer the message in the encrypted format. To preserve the encrypted data similarity search schemes used in the existing system [19] which can successfully exploit by cyber stalkers with known cipher attacks.In the same way, some other approaches are discussed here which are related to cloud performance measurement, cloud applications and cloud platforms, etc.

Ahmad *et al.* [31] specified about importance of cloud-based software services scalability and its technical measurement. Here, considered the elasticity metric as a technical measurement for measuring the performance of a cloud. In this work, authors used two cloud-based systems such as Microsoft Azure and Amazon EC2. It extends to that work has given a comparison report between same cloud software services on the same platform of a cloud with difference scaling policies. Chaudhry *et al.* [32] proposed an authentication scheme; i.e. demand response management scheme (DRMAS). That uses to protect smart grid environment over the cloud infrastructure. The main motive of this work is to reduce the known attacks and improve the efficiency of the utility center. It extends to that helps to secure the transferring data among the connected components over Internet of things (IoT).

Ali *et al.* [33] proposed an improved scheme (iTCALAS) over the temporal credential based anonymous lightweight authentication scheme (TCALAS) [42]. The main objective of this work is reducing the security challenges over Internet of Drones (IoD). Utilization rate of unmanned aerial vehicles increasing day by day due to their portable nature and openness communication architecture. It may cause to increase the cyber-attacks on the sensitive data that is transmitting among

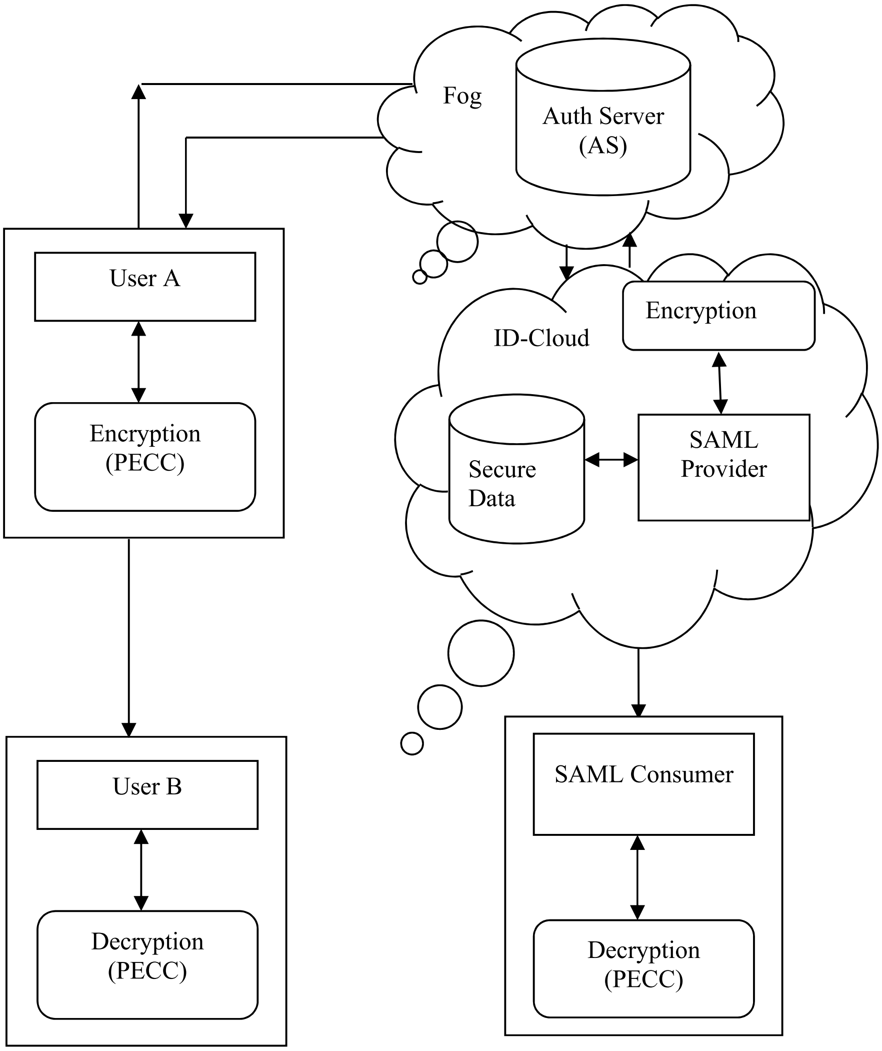

FIGURE 1. Proposed protocol for secure IDaaS.

the IoD connecting devices. iTCALAS gives solutions to the security challenges over IoD.

Abdalla *et.al* [35] proposed an authentication key exchange protocol. It helps to secure the password whenever sharing among multiple parties over a network. To design and developed, the proposed approach, here, authors followed three party scenarios without using Random Oracle Model [41]. In this work authors discussed about in secure 3-party password-based cipher key exchange protocol. As well as described about the security models for two party password based vital exchange. Table 1 shows the comparison among the related works by considering some characteristics like security services, performance measurement and Authentication protocols. Here, the integrity and confidentiality services considered as security services to analyze with the existing approaches. Some authors [31], [39] have used OAUTH and OPEN ID protocols as authentication protocols to verify the communication data and user's identity. In the proposed approach considered SAML as authentication protocol due to its unique factor like SPOA [3]. Table 1 shows proposed system will be provides both the security services.

TABLE 1. Literature survey comparison report.

Approach	Characteristics		
	Security Services	Performance Measurement	Authentication Protocol
[31]	Yes	No	OAUTH
[35]	No	No	No
[36]	No	No	No
[38]	Yes	Yes	No
[39]	No	No	OpenID
[40]	No	No	No
Proposed	Both	Both	SAML

III. ANOMALY DETECTION

It is a cloud based anonymous authentication protocol. The proposed cloud environment consists of some components to provide authentication that includes anonymity based

IDaaS system. Authentication Server, Secure ID Server, SAML Protocol and Pentatope found Elliptic Curve Crypto Cipher (PECC) are the essential components of the proposed cloud based protected authentication protocol as shown in Fig. 1. In the traditional cloud, there are significant security risks which are related to information maintenance among multiple mobile users [18], [23]. For example, a hacker can deploy malware application on any device in the cloud environment based on which location can possible to exploit the vulnerability [8]. Hence, required to adopt a protocol that can able to perform continuous auditing or monitoring the communication along with integrity verify. Let us consider the following things that are pre-requisite to define the cloud based SAML and PECC based anonymous authentication protocol. Each client needs to register to the Fog based authentication server (AS) who wants to participate in the communication. It must be authorized each party before going to join in the communication based on registered information. Necessary client attributes are maintained in protected way using SAML and PECC and holds at cloud server. Next prerequisite is all clients need to communicate via web application and web browser because of presence of components on cloud infrastructure. One more prerequisite is that authentication server and Identity management (ID) server share the attributes to validate and provide the authorization tokens/tickets to the inventors as shown in Fig 2.

Protocol 1 address the authentication dialogues related to Client ‘A’ initiation request to Authentication Server ‘AS’ to get an authentication token from AS. It helps to prove him (Client ‘A’) as an authorised person at Identity based server (IDS) like Zero Knowledge based protocol (ZK protocol) [24], [26] for doing further processing.

With the reference of an authorised encrypted token received from Authentication Server (AS) from Fog environment, Client A takes initiation to get a ticket by proving himself as a trusted registered node at ID server (IDS) which has resided at cloud environment. Protocol 2 addresses the authentication dialogues between Client ‘A’ and IDS. It shows issuing of an authorised encrypted Ticket along with a secret key to Client ‘A’ after done verification. Protocols 3 shows that the authorised parities communication after proved them self to each other as an authorised party with the reference of Ticket (random time stamp based) issued by IDS [24].

In this privacy and preservation communication process, the data never is preserved at any location [17]. Session based communication can reduce the authentication attacks. Hence the requested and verified and issued information always participate with the time slot or nonce. After completion of the session every user should need to prove himself as an authorised person and needs to get a token and ticket if they want to continue the communication. Through this approach can able to reduce ID theft attacks [34], Data loss attacks [38], [39] from the attackers through the breaches of data storage locations [22]. Data can protect from the cyber stalker through PECC [7] and SAML [3] as well as can improve the confusion and diffusion [43] factors by adding session time as an additional feature to the dialogues. It can resist also the forgery attacks by adding session time and double spending authentication verifying process as an integrity checking.

Protocol 1 Initiation Request by User ‘A’

Step 1: Client A desires the Authentication server (AS) with $ID_A||$ Request

$$A \rightarrow AS : ID_A||\mathrm{Request} \tag{1}$$

where $ID_A =$ Identity of Client A
Step 2: AS verifies the ID_A
Step 3: If $ID_A =$ True then:

$$AS \rightarrow A : E_k(\text{AS-IDS})\ (\text{Token})||T_1 \tag{2}$$

where $E_k(\text{AS-IDS}) =$ Encryption Key between AS and IDS
$T_1 =$ Time stamp between AS and Client A.
Step 4: Else: Notify to register in the cloud based AS server and drop the connection.

Note: Client A has no access to the encryption key provided by AS and only IDS sever can decrypt the key.

By getting authorisation from the AS, Client A forwards the request to IDS as follows:

Protocol 2 Zero Knowledge Based (ZK) ID Proof Protocol

Step 1: Client A desires IDS with $ID_A||E_{k(AS-IDS)}||ID_B||T_2$

$$\text{Client A} \rightarrow \text{IDS}: ID_A||E_{k(AS-IDS)}||\mathrm{ID_B}||T_2 \tag{3}$$

where $ID_B =$ Identity of Client B.
Step 2: IDS verifies the request.
Step 3: If True then:

$$\text{IDS} \rightarrow \text{ClientA}: E_{K-SAML}(\text{IDS-B})\ (Ticket)\ ||RK_{A-B}||\ ID_A\ ||ID_B||\ T_3 \tag{4}$$

where $E_{K-SAML}(\text{IDS-B}) =$ Encryption key between IDS and Client A.
$RK_{A-B} =$ Random Key between A and B.
$T_2, T_3 =$ Time stamps between respective server and client.
Step 4: Else: Notify incorrect attributes and drop the connection.

Note: Client ‘A’ has no access to encrypted key provided by IDS, it can only be decrypted by Client ‘B’.

After getting authorised by both the servers, Client A communicates with Client B as follows:

Note: Client B has no access to the encrypted key existing between AS and IDS, it has only access to the key provided between IDS and B, so that B can decrypt it.

Cloud based communication parties based on the proposed method, first sends a request to the authentication server (AS) with its Identity, AS checks the user attributes and if the user is authenticated it sends a token along with the timestamp.

TABLE 2. Comparison analysis.

Process	**OpenID Connect [9,10]**	**OAuth [10]**	**SAML [3]**	**Proposed Protocol**
Authentication and Authorization	It does not provide authorization, but it provides authentication	It provides authorization and pseudo authentication	It provides authorization and authentication	It provides authorization and authentication
Motivation	Single sign on for consumer applications	Meant for API authorization between the applications.	Single sign on for Enterprise user applications.	Identity as a service with security feature with distributed feature.
When to Use	In the mobile applications and while writing a new application it is used.	Best suit for API authorization	It is used in the applications, those support SAML	It can used in all the communications among different kinds of devices.
Protocol	XRDS, HTTP	JSON, HTTP	SAML, XML, SOAP, HTTP	SAML, PECC
Security Consideration	Phishing attack, as it relies on the third party there is a chance of misuse of user credentials by the third party. As well there are some authentication flaws in OpenID	Session fixation vulnerability, where invader fixes a token for the victim that is already authorized, and it is highly insecure because it completely depends on TLS to provide confidentiality	There is a chance of occurring XML signature wrapping vulnerability	XML
Token Format	JSON	JSON or SAML2	Authentication attacked theft attack, forgery and active	XML

Client A is unaware of the encrypted token sent by AS, further it is forwarded to the identity management server (IDS) and the key is decrypted only by IDS using the shared attributes between AS and IDS. It in-turn sends the encrypted ticket and a random key with timestamp to the client A. It transmits the PECC encrypted message to the client B. It has no access to the encrypted ticket. Client B receives the request and to decrypt the message, it gets authenticated by both the servers. This method has been analysed with the existing techniques as discussed in section 4.

IV. COMPARISON ANALYSIS

In this section, the comparisons of proposed protocol with the existing protocols are shown in table 2. The characteristics of the proposed protocol also referred in table 2 such as authentication, Authorisation, Secure communication and Maintenance and Integrity. These characteristics achieved by process of various algorithms like PECC [7], SAML [3], Zero Knowledge (ZK) protocol [24] and Cloud and Fog [32] based data maintenances. This protocol helps to achieve the issues facing in cloud-based communication system by Multi level integrity checking includes in fog computation. But the common technical perspectives considered by the majority of the researchers or academicians are measuring the elasticity of cloud services [32]. Elasticity measures by various factors such as time shares, time length, reconfiguration time, scalability and accuracy in different states (over provisioned and under provisioned).

Along with elasticity also other factors affect the performance of the cloud services such as authentication protocols, integrity checking, and data privacy mechanisms. In this paper, we have given authentication protocols that can enhance the cloud/fog performance in terms of secure communication. It reaches by reducing the cyber-attacks on cloud. And also shows effect on response time for the data communication and data computation. The latency time of proposed protocol evaluated by finding the delay between request of user ‘A’ and response of proposed application. It is also referred as elasticity measurement. It extends to that the communication costs and the communication numbers in the

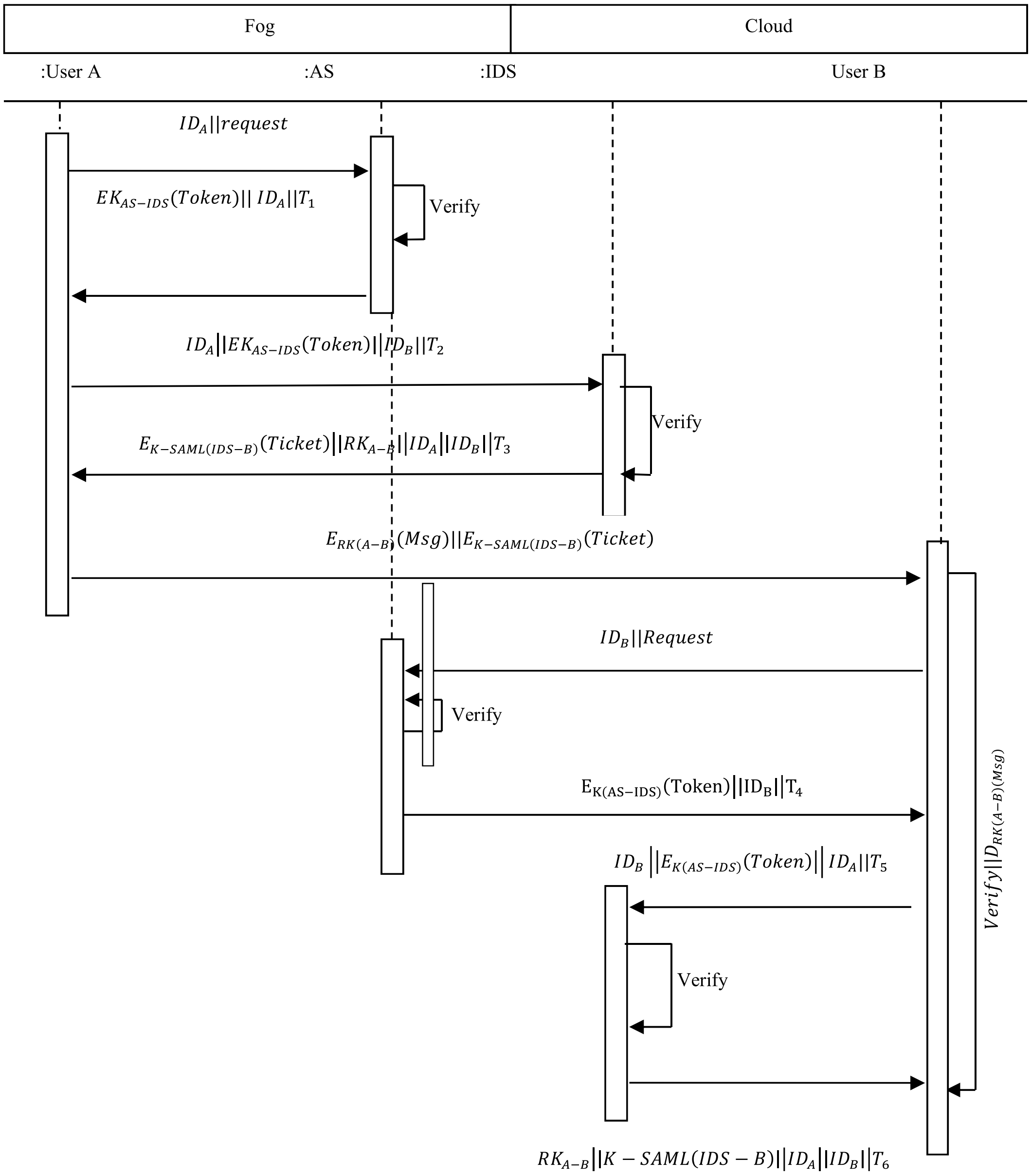
Fog
Cloud
:User A
:AS
:IDS
User B
$ID_A||request$
$EK_{AS-IDS}(Token)|| ID_A||T_1$
Verify
$ID_A||EK_{AS-IDS}(Token)||ID_B||T_2$
Verify
$E_{K-SAML(IDS-B)}(Ticket)||RK_{A-B}||ID_A||ID_B||T_3$
$E_{RK(A-B)}(Msg)||E_{K-SAML(IDS-B)}(Ticket)$
$ID_B||Request$
Verify
$E_{K(AS-IDS)}(Token)||ID_B||T_4$
$ID_B||E_{K(AS-IDS)}(Token)||ID_A||T_5$
Verify
$Verify||D_{RK(A-B)(Msg)}$
$RK_{A-B}||K-SAML(IDS-B)||ID_A||ID_B||T_6$

FIGURE 2. **Flow of transactions.**

proposed protocol is maximum than other protocols. This is caused due to the cloud server should need to verify authenticity of the requests received from clients. The other one is server must securely return an acknowledgment to the client which can helps to integrity checking.

V. RESULTS AND ANALYSIS

To get the computational performance, we simulated the parties' communication using Visual studio 2012, Windows Azure cloud and cloud server. This system performance is better than existing protocols like Lightweight NFC protocol [24], ID based public auditing protocol [5], Uniform Identity Authentication method [1],etc. Computation, Communication, Memory and Time are main important performance metrics a fog application. Computation and communication time are less due to separate cloud environment were maintained for Authentication server and Identity (ID) server. The proposed system is reliable and cost efficient like as shown in Fig.3. Attack rate, Response Time, Computational speed and latency have been considered as functional factors here to test the performance of the proposed protocol. By maintaining the distributed architecture the attack rate (unauthorised accessing) [34] and latency (delay between user action and application) [40] are less comparatively others. By adding authorization and confidentiality approaches like SAML [3], PECC [7], ZK protocols [27] to enhance security to the data communication via cloud and fog where the response time and computation speed affected.

Protocol 3 Authorised Parties Communication

Step 1: Client A transmits the encrypted message to Client B.

Client A → Client B:

$$E_{RK(\text{A-B})}(Msg)||E_{k-SAML(IDS-B)}(Ticket) \tag{5}$$

where $E_{RK(\text{A-B})}(Msg) =$ Encrypted message using PECC from client A to B

Step 2: Soon after receiving the request Client B needs to be authorized in-order todecrypt the message.

$$\text{Client B} \rightarrow \text{AS} : (\text{ID}_\text{B}||\text{Request}) \tag{6}$$

Step 3: AS authenticates ID_B.

Step 4: If $\text{ID}_\text{B} =$ True then

$$\text{AS} \rightarrow \text{Client B: transmits } E_{k(\text{AS-IDS})}\ (Token)||T_4. \tag{7}$$

Else: Drop the connection

Step5: $ID_B \rightarrow$ IDS:transmits

$$E_{k(\text{AS-IDS})}\ (Token)\ ||ID_A||\ ID_B||T_5 \tag{8}$$

Step 6: IDS authorizes ID_B.

Step 7: If $\text{ID}_\text{B} =$ True then

$$\text{IDS} \rightarrow \text{Client B: } RK_{A-B}\ and\ K - SAML_{IDS-B}||T_6 \tag{9}$$

where T4, T5, T6 = Random Time stamp between individual servers and client B.

Step 8: Client B decrypts the message sent from Client A.

Client B: $D_{RK(\text{A-B})}(Msg)$.

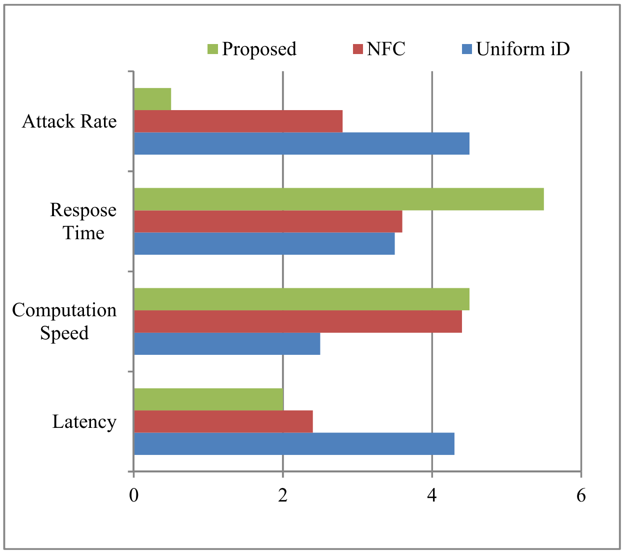

FIGURE 3. Performance analysis using functional factors.

Table 2 and Fig.4 show that response time while transmitting the data over proposed model. This system tested on private cloud, infra stack based. Configuration of this environment is Ubuntu 16.04 LTS (Xenial Xerus) and Linux kernel version 3.13.0 based operating system and Haproxy, Rabbit_mq servers with open stack services.

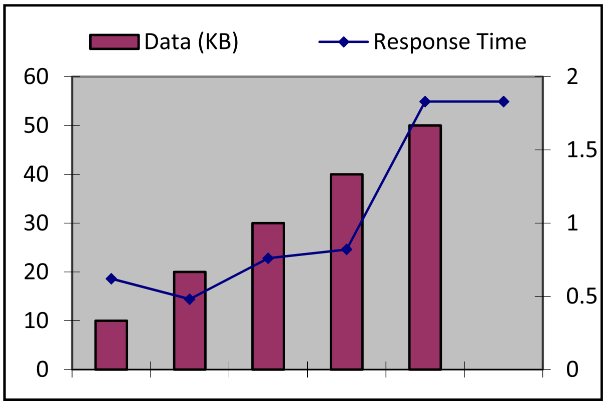

FIGURE 4. Response time for corresponding data computation.

TABLE 3. Response time based analysis.

File size	Response Time (sec)
10kb	0.6213
20kb	0.4842
30kb	0.7650
40kb	0.8243
50kb	1.83

VI. CONCLUSION AND FUTURE SCOPE

The proposed work can improve the cloud features in terms of security through continuous auditing among different communication components. This work main objective is IDaaS based cloud integrity checking protocol development with privacy preservation and authentication features. This protocol can resist even forgery attacks, ID theft attacks and authentication attack through double spending authentication mechanism among Authentication server (AS), Identity management Server (IDS) and users. In future, we would like to enhance this work over the resource limited edge devices like the IoT end devices.

REFERENCES

[1] D. Jing, J. Yan, A. Fujiang, and Z. Ying, "An improved uniform identity authentication method based on SAML in cloud environment," in *Proc. IEEE 3rd Int. Conf. Data Sci. Cyberspace (DSC)*, Jun. 2018, pp. 762–767.

[2] I. Indu, P. M. R. Anand, and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," *Eng. Sci. Technol., Int. J.*, vol. 21, no. 4, pp. 574–588, Aug. 2018.

[3] C. Wang, K. Ding, B. Li, Y. Zhao, G. Xu, Y. Guo, and P. Wang, "An enhanced user authentication protocol based on elliptic curve cryptosystem in cloud computing environment," *Wireless Commun. Mobile Comput.*, vol. 2018, 2018.

[4] R. Parsamehr and S. F. H. Nezhad, "Mutual authentication protocol to share files in cloud storage," in *Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol. (ICCICCT)*, Dec. 2016, pp. 456–461.

[5] H. Jiang, M. Xie, B. Kang, C. Li, and L. Si, "ID-based public auditing protocol for cloud storage data integrity checking with strengthened authentication and security," *Wuhan Univ. J. Natural Sci.*, vol. 23, no. 4, pp. 362–368, Aug. 2018.

[6] J. Shen, D. Liu, Q. Liu, X. Sun, and Y. Zhang, "Secure authentication in cloud big data with hierarchical attribute authorization structure," *IEEE Trans. Big Data*, early access, May 17, 2017, doi: 10.1109/TBDATA.2017.2705048.

[7] V. Nikhila and C. Rupa, "Intensifying multimedia information security using comprehensive cipher," in *Proc. Innov. Power Adv. Comput. Technol. (i-PACT)*, Mar. 2019, pp. 56–61.

[8] B. Varghese and R. Buyya, "Next generation cloud computing: New trends and research directions," *Future Gener. Comput. Syst.*, vol. 79, pp. 849–861, Feb. 2018.

[9] S. Ijaz and E. U. Munir, "MOPT: List-based heuristic for scheduling workflows in cloud environment," *J. Supercomput.*, vol. 75, no. 7, pp. 3740–3768, Jul. 2019.

[10] M. Bilal, M. Asif, and A. Bashir, "Assessment of secure OpenID-based DAAA protocol for avoiding session hijacking in Web applications," *Secur. Commun. Netw.*, vol. 2018, pp. 1–10, Nov. 2018.

[11] I. Indu, P. M. R. Anand, and V. Bhaskar, "Encrypted token based authentication with adapted SAML technology for cloud Web services," *J. Netw. Comput. Appl.*, vol. 99, pp. 131–145, Dec. 2017.

[12] H. Jannati and B. Bahrak, "An improved authentication protocol for distributed mobile cloud computing services," *Int. J. Crit. Infrastruct. Protection*, vol. 19, pp. 59–67, Dec. 2017.

[13] D. M. Shila, W. Shen, Y. Cheng, X. Tian, and A. X. S. Shen, "AMCloud: Toward a secure autonomic mobile ad hoc cloud computing system," *IEEE Wireless Commun.*, vol. 24, no. 2, pp. 74–81, Apr. 2017.

[14] D. Gonzales, J. M. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods, "Cloud-trust—A security assessment model for infrastructure as a service (IaaS) clouds," *IEEE Trans. Cloud Comput.*, vol. 5, no. 3, pp. 523–536, Jul. 2017.

[15] M. Adhikari, T. Amgoth, and S. N. Srirama, "A survey on scheduling strategies for workflows in cloud environment and emerging trends," *ACM Comput. Surv.*, vol. 52, no. 4, pp. 1–36, Sep. 2019.

[16] J. Zhang, Z. Zhang, and H. Guo, "Towards secure data distribution systems in mobile cloud computing," *IEEE Trans. Mobile Comput.*, vol. 16, no. 11, pp. 3222–3235, Nov. 2017.

[17] S. Lins, S. Schneider, and A. Sunyaev, "Trust is good, control is better: Creating secure clouds by continuous auditing," *IEEE Trans. Cloud Comput.*, vol. 6, no. 3, pp. 890–903, Jul. 2018.

[18] E. Munivel and A. Kannmmal, "New authentication scheme to secure against the phishing attack in the mobile cloud computing," *Secur. Commun. Netw.*, vol. 2019, May 2019, Art. no. 5141395.

[19] C. Guo, P. Tian, and C.-C. Chang, "Privacy preserving weighted similarity search scheme for encrypted data," *IET Inf. Secur.*, vol. 13, no. 1, pp. 61–69, Jan. 2019.

[20] Y. Liu, S. Xiao, H. Wang, and X. A. Wang, "New provable data transfer from provable data possession and deletion for secure cloud storage," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, pp. 1–12, Apr. 2019.

[21] A. Choudhary, I. Gupta, V. Singh, and P. K. Jana, "A GSA based hybrid algorithm for bi-objective workflow scheduling in cloud computing," *Future Gener. Comput. Syst.*, vol. 83, pp. 14–26, Jun. 2018.

[22] T. Xiang, X. Li, F. Chen, Y. Yang, and S. Zhang, "Achieving verifiable, dynamic and efficient auditing for outsourced database in cloud," *J. Parallel Distrib. Comput.*, vol. 112, pp. 97–107, Feb. 2018.

[23] Y. Yang, C. Lv, W. Ma, Q. Jiang, and J. Gu, "Security analysis of Kulseng et al.'s mutual authentication protocol for RFID systems," *IET Inf. Secur.*, vol. 6, no. 4, pp. 239–248, Dec. 2012.

[24] K. Fan, C. Zhang, K. Yang, H. Li, and Y. Yang, "Lightweight NFC protocol for privacy protection in mobile IoT," *Appl. Sci.*, vol. 8, no. 12, p. 2506, Dec. 2018.

[25] M. Torquato, I. M. Umesh, and P. Maciel, "Models for availability and power consumption evaluation of a private cloud with VMM rejuvenation enabled by VM live migration," *J. Supercomput.*, vol. 74, no. 9, pp. 4817–4841, Sep. 2018.

[26] M. BaqerMollah, M. A. K. Azad, and A. Vasilakos, "Security and privacy challenges in mobile cloud computing: Survey and way ahead," *J. Netw. Comput. Appl.*, vol. 84, pp. 38–54, Apr. 2017.

[27] J. Bootle, A. Cerulli, E. Ghadafi, J. Groth, M. Hajiabadi, and S. K. Jakobsen, "Linear-time zero knowledge proofs for arithmetic circuit satisfiability," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2017, pp. 336–365.

[28] B. Rashidi, "Authentication issues for cloud applications," *IET Authentication Technol. Cloud Comput., IoT Big Data*, vol. 1, pp. 209–240, Mar. 2019.

[29] L. Xue, J. Ni, Y. Li, and J. Shen, "Provable data transfer from provable data possession and deletion in cloud storage," *Comput. Standards Interfaces*, vol. 54, pp. 46–54, Nov. 2017.

[30] H. Wu, W. Zheng, and A. Chiesa, "DIZK: A distributed zero knowledge proof system," in *Proc. 27th USENIX Conf. Secur. Symp.*, 2018, pp. 675–692.

[31] A. A.-S. Ahmad and P. Andras, "Scalability analysis comparisons of cloud-based software services," *J. Cloud Comput.*, vol. 8, no. 1, p. 10, Dec. 2019.

[32] S. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: A certificate based authentication scheme for smart grid access control," *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[33] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020.

[34] C. Rupa, G. T. Reddy, M. H. Abidi, and A. Alahmari, "Computational system to classify cyber crime offenses using machine learning," *J. Sustainability*, vol. 12, no. 10, pp. 1–15, 2020.

[35] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Proc. Int. Workshop Theory Pract. Public Key Cryptogr. (PKC)*, in Lecture Notes in Computer Science, vol. 3386. Cham, Switzerland: Springer, 2005, pp. 65–84.

[36] G. T. Reddy, M. P. K. Reddy, K. Lakshmanna, R. Kaluri, D. S. Rajput, G. Srivastava, and T. Baker, "Analysis of dimensionality reduction techniques on big data," *IEEE Access*, vol. 8, pp. 54776–54788, 2020.

[37] M. Kamal and M. Tariq, "Light-weight security and blockchain based provenance for advanced metering infrastructure," *IEEE Access*, vol. 7, pp. 87345–87356, 2019.

[38] C. Iwendi, Z. Jalil, A. R. Javed, T. G. Reddy, R. Kaluri, G. Srivastava, and O. Jo, "KeySplitWatermark: Zero watermarking algorithm for software protection against cyber-attacks," *IEEE Access*, vol. 8, pp. 72650–72660, 2020.

[39] C. Rupa and D. J. Kumari, "Network-based adaptation of blockchain technology," *Int. J. Innov. Technol. Exploring Eng.*, vol. 8, no. 9, pp. 141–148, 2019.

[40] M. U. Abbasi, A. Rashad, A. Basalamah, and M. Tariq, "Detection of epilepsy seizures in neo-natal EEG using LSTM architecture," *IEEE Access*, vol. 7, pp. 179074–179085, 2019.

[41] S. A. Chaudhry, K. Yahya, and F. Al-Turjman, "Correctness of an authentication scheme for managing demand response in smart grid," in *Smart-Grid in IoT-Enabled Spaces—The Road to Intelligence in Power*. New York, NY, USA: Taylor & Francis, 2020.

[42] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment," *IEEE Trans. Veh. Technol.*, vol. 68, no. 7, pp. 6903–6916, Jul. 2019.

[43] D. Ravichandran, S. Fathima, V. Balasubramanian, A. Banu, Anushiadevi, and R. Amirtharajan, "DNA and chaos based confusion-diffusion for color image security," in *Proc. Int. Conf. Vis. Towards Emerg. Trends Commun. Netw. (ViTECoN)*, Vellore, India, Mar. 2019, pp. 1–6, doi: 10.1109/ViTECoN.2019.8899483.

CH. RUPA (Senior Member, IEEE) is currently working as a Professor with VRSEC (A), Vijayawada. She published more than 70 articles in various journals and conferences. Her main research interests include information security, image processing, and security algorithms. She was a Life Member of CSI, ISTE, IAENG, IEI, and IACSIT. She was awarded the Young Engineer of 2010 by JNTU Kakinada. She was awarded the National Young Engineer of 2011 by IEI, Government of Andhra Pradesh, and the Young Engineer of 2012 by IEI. She has received couple of awards from IETE and IEI(I), for her work.

RIZWAN PATAN received the B.Tech. and M.Tech. degrees from Jawaharlal Nehru Technological University, Anantapur, India, in 2012 and 2014, respectively, and the Ph.D. degree in computer science and engineering from the School of Computer Science and Engineering, VIT University, Vellore, India, in 2017. He has been an Assistant Professor with the Department of Computer Science and Engineering, Velagapudi Ramakrishna Siddhartha Engineering College, Vijayawada, India, since 2019. He was a Former Assistant Professor with the School of Computing Science and Engineering, Galgotias University, New Delhi, India, from 2017 to 2019. He has published reputed 20 SCI journals and ten free Scopus indexed journals, and also presented paper in national/international conferences, published book chapters in CRC Press, IGI global, and Elsevier, and an Edited as books. He holds ten Indian patents and one U.S. patent. He received the award from World Research Council and American Medical Council in the title of Innovative Researcher on Big Data and IoT for the year 2019. He is a Guest Editor of the *International Journal of Grid and Utility Computing* (Inderscience), *Recent Patents on Computer Science*, *Informatics in Medicine Unlocked* (Elsevier), and *Neural Computing and Applications* (Springer).

FADI AL-TURJMAN (Member, IEEE) received the Ph.D. degree in computer science from Queen's University, Kingston, ON, Canada, in 2011. He is currently a Full Professor and the Research Center Director of Near East University, Nicosia, Cyprus. He is the leading authority in the areas of smart/intelligent, wireless, and mobile networks' architectures, protocols, deployments, and performance evaluation. His publication history spans over 250 publications in journals, conferences, patents, books, and book chapters, in addition to numerous keynotes and plenary talks at flagship venues. He has authored and edited more than 25 books on cognition, security, and wireless sensor networks' deployments in smart environments, published by Taylor & Francis, Elsevier, and Springer. He has received several recognitions and best papers' awards at top international conferences. He also received the prestigious Best Research Paper Award from Elsevier *Computer Communications* journal for the period 2015–2018, and the Top Researcher Award for 2018 at Antalya Bilim University, Turkey. He has led a number of international symposia and workshops in flagship communication society conferences. He currently serves as an associate editor and the lead guest/associate editor for several well reputed journals, including the IEEE COMMUNICATIONS SURVEYS AND TUTORIALS and *Sustainable Cities and Society* (Elsevier).

LEONARDO MOSTARDA (Member, IEEE) received the Ph.D. degree from the Computer Science Department, University of L'Aquila, in 2006. He is currently an Associate Professor and the Head of the Computer Science Department, Camerino University, Italy. He cooperated with the European Space Agency (ESA) on the CUSPIS FP6 Project, to design and implement novel security protocols and secure geo tags for works of art authentication. To this end, he was combining traditional security mechanisms and satellite data. In 2007, he was a Research Associate with the Distributed System and Policy Group, Computing Department, Imperial College London, where he was working on the UBIVAL EPRC Project in cooperation with Cambridge, Oxford, Birmingham, and UCL for building a novel middleware to support the programming of body sensor networks. In 2010, he was a Senior Lecturer with the Distributed Systems and Networking Department, Middlesex University, where he founded the SensoLab, an innovative research laboratory for building energy efficient wireless sensor networks.