Fingerprint Based Authentication Architecture for Accessing Multiple Cloud Computing Services using Single User Credential in IOT Environments

Biniyam Alemu\textsuperscript{1}, Rajesh Kumar\textsuperscript{2}, Deepak Sinwar\textsuperscript{3}, Ghanshyam Raghuwanshi\textsuperscript{4}

\textsuperscript{1,2}Department of Computer Science, Bule Hora University, Ethiopia
\textsuperscript{3,4}Department of Computer and Communication Engineering, Manipal University Jaipur, India

Corresponding author: Deepak sinwar (deepak.sinwar@gmail.com)

Abstract. Cloud computing technology provides access to the pool of configurable resources including storage space, application, services and on demand network. Involvement of Cloud with the organization minimizes organization efforts toward fulfilling its customer’s needs. One of the major advantages of cloud computing is the Single Sign On (SSO) technique that allows the user to access multiple application services using a single user credential. In cloud computing, there are many issues, and challenges to be discussed. However, prevention from security attacks is much more difficult in preserving privacy of user agents. This paper has proposed SSO-based bio-metric authentication architecture for cloud computing services to overcome the security and privacy attacks. Bio-metric authentication is effective for resources controlled by end devices at the time of accessing the cloud services since these devices are computationally inefficient for user information processing during authentication. Accordingly, security attack in the cloud computing gets minimized using the proposed architecture. The proposed architecture also includes a novel approach in which there exist one to one relationship between user agent and the service provider. In this user agents can use their fingerprint while requesting for registration and accessing different cloud application services at cloud. Based on comparative study with several existing architectures, the highlights of the proposed architecture have been presented.

1. Introduction
Cloud computing enables convenient and on demand network access to the shareable and configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released through service provider interaction [1]. In this, service providers are distributed over the world and the number of these service providers is growing rapidly for providing sufficient resources and storage space at cloud to the users.

While accessing different independent Cloud services in the Cloud Computing environment, there is a concept of Single Sign-On (SSO) technique. It is a technique that let a user only to have single login account and can access all authorized services in the Cloud environment using single sign in [2]. This technique is assumed to be more reasonable, and competent in many services operated by Cloud environment [3]. In addition to this, SSO offers the advantages of user account management which is independent on Cloud environments [4]. Method [5] proposed the solution for this issue and it can also
reduce the expected cost for each user to have user credential. According to Hwang et.al [6], there are three popular authentication mechanisms for SSO:

1.1. Kerberos
Kerberos is the type of authentication protocol which consists of a trusted third party and a key distribution center (KDC). This method generates the ticket as an identity for obtaining the permissions of the cloud. The major loophole in the Kerberos mechanism is the involvement of third party in authentication process and KDC involve in sharing key for authentication purpose. If there is failure of Key Distribution Center (KDC) then it also results in delay with authentication mechanism.

1.2. Smart card
Secret information of user agents is store in a smart card. Registration entity provides a user encrypted smart card with the help of smart card making machine. Encrypted smart card is used by user in the CSP login service portal. It can reduce the user’s authentication time without any need of storing and protecting many authenticate information.

1.3. One Time Password (OTP)
OTP is a two-factor authentication technique which works for the authentication of user verification. Now a days, digital banking technology provides OTP authentication mechanism to verify the authenticity of the user. An OTP is generated on user’s registered mobile number and there is timespan for that OTP. It needs two key states, password, and physical token for working together. Basically, it is owned by the user and It can be changed dynamically based on the allocated time span for token and it uses pseudo-number generator algorithm for authentication purposes. However, all these three mechanisms for authentication of SSO have security loopholes. SSO independent Cloud services are going to be accessed using only a single user credential. But, in this scenario, if the user credential is compromised once then the user may lose everything on the Cloud. Therefore, rather than use of smart card, OTP, and Kerberos etc. for SSO purpose, it is better to use the Biometric authentication mechanism because it is hard to break the security of a biometric system over other authentication techniques.

Biometrics authentication technique is an approach that uses the unique patterns of either physical or behavioral traits of users for authentication purposes [7]. According to the method [8], it is highly consistent since the physical physiognomies of human beings are much more challenging to be counterfeit than other security codes like passwords and hardware keys. This authentication technique is applicable in single sign-on, data protection, remote access to resources, and web security application areas. This technique is rapidly increasing and replacing traditional password and token-based authentication systems. According to the method proposed in [9], there are some biometric traits that can be defined for an individual, like fingerprint, hand palm, iris, voice, face, and so on. Comparing fingerprint with other biometric technologies like face, iris, and voice it has been observed that fingerprint-based recognition broadly used. For a fingerprint-based technology, the pattern is determined after birth, and different fingerprint patterns are owned by even identical twins [7]. Even though fingerprint based is secured compared to other biometric based authentication mechanisms, but it also has some flaws, and which cannot be claimed for fully secured system.

To access Cloud Services, users are supposed to go through public internet environment. These environments are vulnerable to several malicious attacks. Among these malicious attacks, Distributed Denial of Service (DDoS) attack, password spoofing, and message interception are the most important attacks which need to be discussed in the area of Cloud Computing Services, since it uses resource constrained devices while providing services and applications for users. In addition to this, there are multiple numbers of service providers in Cloud Computing and due to this reason, user account management is also another issue. End devices used for accessing Cloud based services are resource constrained and so they are computationally inefficient. In [16], the issue of DoS attack was tried to be handled by status bit of 0 (when user logged out) and 1 (when user logged in) but what about the case
when a single user is attacking the cloud services through multiple registrations using different ID which results in too busyness in network and data accessibility through DDoS attack. It is another issue which needs to be discussed. Therefore, security mechanisms which could improve the performance of the method [16] and could deal with the DoS attacks along with the issues like smart card lost and password interception should be proposed.

In this paper, proposed method deals with the fingerprint-based authentication framework to get rid of the security and privacy attack toward Cloud Computing environment. In addition to reducing security attack, it is also suitable for resource constrained end devices which are used for accessing the services, and it is the easiest way of account management for accessing multiple application services with a single credential for applying the concept of Single Sign-On (SSO). The rest of the paper is organized as follow: section 2 discusses about the related work of the authentication framework in cloud environment. Section 3 discusses about the proposed fingerprint-based architecture of authentication mechanism and their working procedure. Section 4 discusses about the security and functionality analysis of the proposed scheme and section 5 about conclusion of the paper.

2. Related Work
After the evolution of Cloud Computing, several authentication mechanisms to access Cloud based services have been proposed. According to [6], the concept of SSO is discussed which is based on smart card scheme for accessing multiple cloud services. In this paper, the authors addressed the problem with Kerberos and OTP based SSO mechanism. The Kerberos based technique has a defect that the authentication cannot be processed if the Key Distribution Server (KDC) becomes offline. The problem with OTP based SSO technique is that the user cannot pass the authentication forever if the physical token is lost. This paper proposed Trust Server (third party) at which user register an account and obtains a smart card for login to access the services of the Cloud. Upon requesting for login to the Cloud, the Cloud sends the user information to the Trusted Server for processing the user request. Upon reception of the message, the Trusted Server will identify the users. In this algorithm, if the user is registered and information is matched then only, the user will be authenticated to access the Cloud services. The issue to be discussed in this paper is that an attacker can extract information of the user from smart card and it can be used for fraud authentication. Another notable work is the one discussed in [10]. According to this method [10], there are masquerade attacks with stolen card, flooding of phone and Login failures on password change problems. The paper proposed hashing function algorithm with one-time key to be transmitted and password change facilities. But such security mechanism is not advisable for resource constrained end devices which are used in Cloud environment. However, hashing function needs high computational processing which results in lower and inefficient functionality of computing devices. A survey in [11] investigated the security and privacy issues of the recent Cloud Computing provisioned by different service providers. According to the investigation, nowadays, security and privacy provided by service providers are not adequate, and this results in vulnerability of user account while accessing the Cloud Computing services. Therefore, further discussion, and improvement towards the security and privacy of the Cloud Computing should be the next target. According to [12], text-based password scheme is a quite weak authentication method for the Cloud environment even if its ease of use due to vulnerabilities such as dictionary and brute-force attacks, and social engineering. In this paper, three level authentication technique is discussed which includes OTP and two-factor authentication using password generator. The main problem with this approach is that OTP can be intercepted, in addition to this, the algorithm is not recommended for resource constrained end devices used in Cloud Computing environment.

Method proposed in [13] discussed that, to relieve the difficulty of managing password and enhance the usability of authentication systems, biometric authentication has been broadly studied and has implemented in academia and industry areas. However, the existing systems could be vulnerable to attacks, which seriously minimize their acceptance by end users. The authors reviewed the recent advances in the field of biometric authentication and found that most of the existing systems suffer
from security and privacy issues. Based on this survey, improving the security and privacy of biometric authentication mechanism is so important. A secure smart card authentication and authorization framework using in Multimedia Cloud is discussed in [14]. There is account management and changing user permission issues in distributed Cloud environment. From attacker’s point of view, the problem with this algorithm is that an attacker can extract information of the user from smart card and can be used it for authentication.

According to [15] authentication mechanism to access multiple applications using single credential is discussed in the area of Internet of Things. Since the algorithm discussed in this paper is exponential computation, this not recommended for resource constrained end devices of Internet of things. The recent research conducted on achieving the security of Cloud Computing discussed in [16]. Accordingly, user’s credentials pass via communication environment which is vulnerable for a number of malicious attacks, also they are susceptible to identity tracing, and masquerade attacks, and as well as end devices that are used while accessing the service resource constrained. The authors proposed a smart card-based framework that allows Single Sign-On (SSO) mechanism to access multiple cloud services using a single account. But attacker can extract information of the user from smart card and use it for authentication. In addition to this, during authentication process, still there are masquerade and identity tracing attack in the proposed solution since the framework is hardware based. Kok-seng wong et al [17] discusses about the secured biometric authentication protocol for cloud computing, here author mentions modeling about biometric authentication procedure, calculation and verification of vector which is responsible for biometrics traits, encryption modules Processing power in the verification process, is the major concerned regarding any biometric verification.

Issues with the existing approaches:
1. Attacker can extract information of the user from smart card with the help of skimming device and can be used for authentication.
2. If smart card of the user is lost, then the user cannot be authenticated forever.
3. OTP generated by service provider can be interrupted by an attacker and used for authentication.
4. One-time registration is used only for removing the redundancy of user id, but still there is a DOS attack which can be done through one user per multiple registrations on the cloud.
5. If the smart card of the user is lost, then the user may lose all the information stored on the cloud.
6. Adding password change facility to the existing scheme is another workload for IoT end devices.
7. Smart card production process requires exponential computation, which is not good for resource constraint IoT devices.
8. Since the framework is hardware based [9], during authentication process, still there is masquerade and identity tracing attacks in the above-mentioned solution.

3. Proposed Architecture
This paper proposes fingerprint-based authentication framework to relieve the security and privacy attack toward Cloud Computing environment. In addition to reducing security attack, it is also suitable for resource constrained end devices which are used for accessing the services, and it is the easiest way of user account management for accessing multiple application services which apply the concept of Single Sign-On (SSO). The framework could implement in Social Media platforms that prevent duplication of the users from registering especially for Facebook and Twitter and current framework can be used in removing the user account redundancy and fake accounts. Following entities are involved in the proposed Architecture:
1. **User**: A person who requests for the use of services on the Cloud
2. **Client**: A workstation, computer, or device that is connected with internet and having fingerprint scan technology. Biometric Sensor, scans user fingerprint using fingerprint scan
technology and a feature extractor process which scans the biometric data to extract the feature vector as given in (1)

\[ X = (x_1, x_2, x_3, x_4, \ldots, x_n) \]  

3. **The encryption module**: It is responsible for encrypting requests using private key of the user EPrue(X), Hash password h(pwd) and User id (Ui) which is encrypted with RVS public key and it is send to the RVS using registration request. When client wants to login in to the Cloud Service Provider (CSP), then the secured information is calculated as given in (2).

\[ S = (\text{EPucsp}(\text{Ui})(\text{EPru}(X))) \]  

4. **Registration & Verification Server (RVS)**: Responsible for the registration and verification of the users and cloud services.

4.1 **Registration Process**: Secured information S can be calculated using RVS private key and public key of the user as given in (3).

\[ S = (\text{DPrrvs}(\text{Ui})h(\text{pwd})(\text{Dpuu}(X))) \]  

Where, 
- S= secured information received form user 
- Ui= User Identity 
- h= collision free one-way hash function 
- DPrrvs= Decryption using Private Key of the Registration and Verification Server 
- Dpuu= Decryption using public key of the user 

When RVS receives registration request form client, it captures a user identity that is decrypted using rvs private key, hash password, encryption module that RVS Decrypt using client public key and it is processed through transform via verification module and saves into its database in the form of template. In the response RVS, registration response is provided to the client using secure channel. Cloud services can be available to anyone by sending the SIDj (Cloud Service provider identity) to RVS, which is verified and as a result, trust certificate is provided to the client.

4.2 **Verification Process**: Verification server responsible for verifying the identity and fingerprint of the user. When CAS forward request of the user to verification server it matches Si =Sj, here Si is the secured information sent by user at the time of registration and Sj is the secured user information received by CSP. If the information is verified it send authentication response to CAS.

5. **Login Server (LS)**: It provides an interface to access the Cloud services for the user. If a user wants to access the cloud services, then he/she can use his fingerprint and user id (Ui) to the cloud service portal for login. The login server, forwards request to authentication server for verifies legitimacy of the user using S as given in (4)

\[ S = (\text{EPucsp}(\text{Ui})(\text{EPru}(X))) \]  

6. **Authentication Server (AS)**: It verifies the user, who trying to log in into the Cloud. CAS Decrypt (Sj= (DPresp(\text{Ui})(Dpuu(X))) and matches Ui and (X) which are already stored in their database. If the request is first time made, then the system forwards the request for RVS. If the AS received authentication response from RVS and user is authenticated user, then it set the status bit=1. If the request sent by user is not first time, then it will check in their database, it matches Ui with already store Ui and status bit corresponding to the user is checked. CAS send OTP to the user along with trust certificate, then user enters the OTP and server verifies his identity and set the status bit of corresponding user to 1.

7. **Application Server (AS)**: Provides the required application, services, and data to the users.

8. **IoT Devices**: Several type of IoT devices which are available at the user/server end provides real time data to the cloud servers.

3.1. **Working procedure**

Users, who want to access the cloud services for first time need to place a request to the registration and verification server using his fingerprint scan, hash password and registration details. Client is responsible for retrieving the fingerprint scan and feature extractor identifies and extracts the unique
feature of the fingerprint. These extracted features are encrypted with the encryption key and send to the registration and verification server through the secure channel. Registration and verification server receive this encryption module and does transformation and vector calculation and check whether the user already exists or not, if user does not exist then the information will be stored in the form of the template. Cloud services are also registered with the registration and verification server using a secure channel with registration request and response. After registration is done, user can send a login request using his registered finger scan on biometric device. The client is responsible for scan and then after feature extraction module is there followed by encryption module. It further sends a login request to the CSP Login server. Login Server forwards the request to the Cloud Authentication Server for authenticating the details of the user. Authentication Server send this fingerprint template to registration and verification server if the user requested first time to the Cloud Services, otherwise Authentication Server authenticate itself, if the user is not new by checking and setting status bit. Registration and verification server receive request form CSP for verification of the user, it will match the template with already stored module in their database, if the match found it will verify user credentials and send to CSP using secure channel. Once the user is verified, Authentication Server provides access to cloud services which are applicable to that specific user. So, the user can place a single login request, if the request is granted then the user can use multiple Cloud Services using single Sign-On (SSO). In case, if user wants to change his fingerprint number then he can request to the RVS by using his password credential. The RVS request for old credential will be verified and new entry of the fingerprint will be stored in the database. The proposed architecture is depicted in the figure 1. The architecture is based on several registration and authentication algorithms which are discussed in upcoming sub sections.
3.2. User Agent Registration Algorithm
In this algorithm, users will be registered at Registration & Verification Server (RVS) as shown in figure 2. User first provides biometric authentication in the form of fingerprints to RS, which are further verified from the database. If same fingerprints are already existing in the RS then RVS denies the agent registration request, otherwise fingerprints are saved in the database and registration proceeds with success.

```
INPUT: Users Provide Private Information
    USER PROVIDE FINGERPRINT TO RS
    IF (FINGER_PRINT == EXIST)
        RVS DENY USERS
    END IF
    ELSE IF (NEW_USER == TRUE)
        RVS SAVE FINGER_PRINT
        REGISTRATION SUCCESSFUL
        RVS FORWARD TO AS
        THEN,
        AS SAVE THE_INFO ON ITS_DB
    END ELSE IF
    ELSE
        GO_TO_END
    END ELSE

OUTPUT: Users Registered
```

Figure 2: Algorithm for user agent registration

3.3. Authentication Algorithm
This is a second algorithm and it deals with how the user is going to be authenticated and verified. As shown in figure 3, user provides its biometric authentication-based information to the AS. Based on the authentication information stored inside databases at AS, the decision about the authentication is carried out.

```
INPUT: Users provide Login Information
    USER PROVIDES PRIVATE_INFO TO AS
    IF (FINGER_PRINT == TRUE)
        IF (STATUS_BIT == 0)
            STATUS_BIT = 1;
            USER IS ALLOWED;
        END IF
        ELSE
            USER IS DENIED
        END ELSE
    END IF
    ELSE
        USER IS BLOCKED
    END ELSE

OUTPUT: Users Logged into the Cloud
```

Figure 3: Authentication algorithm
3.4. Service provider Registration Algorithm

The registration for the service providers is done based on registration id sent by the cloud service provider to RVS. The RVS then verifies the cloud and provides a trust certificate as shown in figure 4.

| INPUT: Service Provider Request for Registration |
|-----------------------------------------------|
| CLOUD SENDS REGISTRATION ID TO RVS |
| RVS VERIFIES THE CLOUD AND PROVIDE TRUST CERTIFICATE |
| RVS FORWARDS THE CLOUD INFO TO AS |
| OUTPUT: Service Provider Registered |

Figure 4: Algorithm for service provider registration

3.5. Service Access Algorithm

The service access algorithm keeps track of the login information i.e., status of login and logout time and duration. Based on user requirements, the algorithm can be expanded to hold more information i.e., authentication key, resource accessing from the service provider, etc. The general service access algorithm is shown in figure 5.

| INPUT: Login Information |
|--------------------------|
| IF (LOGIN == TRUE) |
| STATUS_BIT = 1; |
| END IF |
| ELSE IF (LOGOUT == TRUE) |
| STATUS_BIT = 0; |
| END ELSE IF |
| ELSE |
| USER BLOCKED |
| END ELSE |
| OUTPUT: Accessing Cloud Services |

Figure 5: Service access information algorithm

4. Security and Functionality Analysis

The proposed architecture is compared with several existing architectures viz. Gupta and M. Quamara [16], and other existing methods. Based on the comparative study, few possible outcomes of the proposed architecture are mentioned as follows:

- Vulnerability of cloud computing to security and privacy attack is minimized due to biometric authentication and use of public key cryptography.
- Architecture is suitable for resource constrained end devices used in cloud computing environment since there is no high processing of information, and exponential computation process during authentication, and no additional workloads, like password change.
- Delay introduced in the previous works is due to the failure of trusted third-party server. However, it can be reduced in proposed architecture, because registration process of using biometric is simple as compared to the other techniques and trusted third party is not going to be participated during authentication.
- Single user agent can only have a single account for multiple cloud application services which removes fake user accounts or redundant account at cloud. There is one to one relationship between user and cloud service.
There is no loss of stored information at the cloud (if the smart card of user is lost) using biometric approach; user can change their fingerprint choice in the RVS using their secured password.

- User can easily change their finger number choice by placing a request to RVS using his password.
- RVS does not involve every time in authentication of the user, therefore the complexity of computational is decreased.
- If an attacker tries to reproduce the fingerprint using mark traced print, then he cannot access the services through mutual authentication because OTP is sent to the devices of registered users only.
- Use of status bit prevents malicious user to log in with the same user credentials multiple times, so the DOS attack is minimized.

5. Conclusion
Cloud computing service providers are circulated all over the domain and their number is increasing rapidly to provide the facilities of adequate resource computation and storage to the users. This paper discusses the background of achieving security in Cloud computing by using biometric mechanism specifically, using fingerprint-based authentication. According to the architecture introduced, security attack occurred in the cloud computing can be reduced as well as fake accounts can be removed by proving the fingerprint-based authentication in the registration process. Proposed technique can be recommended for accessing the cloud services using the resource constrained end devices because the proposed algorithm provides single SSO login and uses multiple cloud application services. But still there is also an issue of vulnerability in fingerprint-based authentication mechanism because users can leave their own fingerprint on any surface, and attackers may use the surface for authentication purposes. The issue of vulnerability can be resolved by introducing the pulse rate of the finger. In future, the validation of the proposed architecture may be conducted by implementing the framework and performance analysis using AVISPA.

References
[1] T. Dillon, Chen Wu, E. Chang, “Cloud Computing: Issues and Challenges,” IEEE International Conference on Advanced Information Networking and Applications, pp. 27-33, 2010.
[2] J. Weiskotten, “Open id single sign on adding authentication to your web applications,” Dr. Dobb’s Journal, Vol. 33, no. 10, Oct. 2008.
[3] S. Fugkeaw, P. Manpanpanich, and S. Juntapremjitt, “Multi-application authentication based on multi-agent system,” IJCS, Vol. 33, no. 2, pp. 37-42, 2007.
[4] D. Nobayashi, Y. Nakamura, T. Ikenaga, and Y. Hori, “Development of single sign-on system with hardware token and key management server,” IEICE Trans. Inf. and Syst., pp. 826-35, 2009.
[5] A. Volchkov, “Revisiting single sign-on a pragmatic approach in a new context,” IT Pro, 2001.
[6] Hwang, M.S., & Sun, T.H. “Using smart card to achieve a single sign-on for multiple cloud services.” IEEE Technical Review 30(5): 410-416, 2013.
[7] W. Yang, S. Wang, J. Hu, G. Zheng, C. Valli, “Security and Accuracy of Fingerprint-Based Biometrics: A Review,” Journal of Symmetry, 2019.
[8] S. R. Kodituwakku, “Biometric Authentication: A Review,” International Journal of Trend in Research and Development, Volume 2(4), pp. 113-123, 2015.
[9] N. Riaz, A. Riaz, S. Khan, “Biometric template security: an overview,” Sensor Review, 2017
[10] Chen, N., & Jiang, R. “Security analysis and improvement of user authentication framework for cloud computing.” Journal of Networks 9(1): 198-203, 2014.
[11] S. Kumar, R. H. Goudar, “Cloud Computing Research Issues, Challenges, Architecture,
Platforms and Applications: A Survey,” International Journal of Future Computer and Communication, Vol. 1, No. 4, December 2012.

[12] Abdellaoui, A., Khamlichi, Y.I., & Chaoui, H. “A novel strong password generator for improving cloud authentication.” Procedia Computer Science 85: 293-300, 2016.

[13] Zhang Rui, Zheng Ya, “A Survey on Biometric Authentication: Toward Secure and Privacy Preserving Identification,” IEEE Access, Volume 7, January 16, 2019.

[14] Yang, T. C., N. W., Liaw, & Wu, W. C. “A secure smart card authentication and authorization framework using in multimedia cloud.” Multimedia Tools and Applications, 11715-11737, 2017.

[15] Bai, T. D. P., Raj, K. K. M., & Rabara, S. A. “Elliptic curve cryptography based security framework for Internet of Things (IoT) enabled smart card.” World Congress on Computing and Communication Technologies (WCCCT) IEEE 43-46, 2017.

[16] Gupta, & M. Quamara, “An identity based access control and mutual authentication framework for distributed cloud computing in Internet of Things environment.” ICCIDS Procedia Computer Science, 189-197, 2018.

[17] Kok-Seng Wong and Myung Ho Kim, “Secure Biometric-Based Authentication for Cloud Computing” Springer International Publishing Switzerland CLOCER 2012, CCIS 367, pp. 86–101, 2013. DOI: 10.1007/978-3-319-04519-1_6.