

Three-Tier Role-Based Authentication with RC-SSO and Mobile Secret Code Access

S.Shiny^{1*}, R. Megiba Jasmine², P.Libin Jacob³, M. Saravana Karthikeyan⁴

¹Assistant Professor (Senior Grade), Department of Artificial Intelligence and Data Science, Mepco Schlenk Engineering College, Sivakasi - 626005

²Assistant Professor, School of Computing, SRM Institute of Science and Technology Tiruchirappalli, Tamil Nadu, India.

³Assistant Professor, Presidency School of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka-560119, India.

⁴Associate Professor, School of Computing, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamilnadu, Pincode -600062

KEYWORDS:

Multi-layer authentication,
Confidential passcode,
Role Integrated Certificate-
Single Sign-On,
Graphical user interface

ARTICLE HISTORY:

Received: 10.11.2025

Revised: 14.02.2026

Accepted: 07.03.2026

DOI:

<https://doi.org/10.31838/NJAP/08.02.22>

ABSTRACT

The goal of this paper is to show how to create a more secure and advanced authentication mechanism. Because technology is evolving at a rapid pace, security techniques such as authentication schemes must be updated as well. For multi-layer authentication, a user doesn't have to provide passwords. As a third-tier authentication code, we're employing the mobile secret code. In order to obtain access to a particular service, that code word is only available for a limited time. With the confidential passcode, we supply the session duration. After the session duration has passed, the user will be unable to utilize the confidential passcode to access the desired service. Another secret code is required for the user to gain access to the desired service. To widen the scope of user authentication, we've incorporated a smartphone code word as a third-tier authentication code for the first time. As a result, we devised a multi-tier authentication scheme based on unified login system to authorized platforms as a solution to this problem. Three-tier authentication security uses login details, and also pattern recognition and one-time passwords (OTP).

Author's e-mail: shynysajai8@gmail.com, megiba.jaz88@gmail.com, libin@presidencyuniversity.in, professorsksaran@gmail.com

Author's Orcid id: 0009-0002-6917-9435, 0000-0002-5691-603X, 0009-0000-8595-330X, 0009-0003-4249-2445

How to cite this article: Shiny S et al, Three-Tier Role-Based Authentication with RC-SSO and Mobile Secret Code Access, National Journal of Antennas and Propagation, Vol. 8, No. 2, 2026 (pp. 259-271).

1. INTRODUCTION

The cloud computing framework enables access to data and digital services by delivering computational resources (e.g., online file storage, social media platforms, web-based email, and cloud business applications), facilitating the use of tailored software and third-party hardware for remote locations. Since the previous couple decades, cloud computing security has become a key subject of study. Cloud networks are exposed to a wide range of assaults and security threats. Before granting users access to cloud resources, the cloud server must identify them. Authentication methods perform main part in identifying passwords, biometrics verification, public

key infrastructure (PKI) and key-based authentication system. RC-SSO verification methods are insecure and vulnerable to attacks such as Man-in-the-Middle and dictionary-based attacks. When users are given the option to choose their own passwords, they choose passwords that are simple to remember and can be rapidly guessed. The technique of proving "who you are" is known as authentication. In the case of email, information security is required in order to communicate with the intended user. Details such as user authentication parameters, recipient contacts.

In contrast to first- and second-tier authentication, third-tier authentication does not require the user to provide authentication credentials. As a third-tier authentication code, we're employing the smartphone

code word. To acquire access to the requested service, this secret code is only available for a limited time. The time duration is set for the confidential passcode, hence user can't be able to access once the time limit expires. Another secret code is required for the user to gain access to the desired service.

Triple-layer authentication (TTA) is a security mechanism used to access resources like applications, digital profiles, or VPNs with multiple factors of authentication needed from the user. Being an essential component of a strong identity and access management (IAM) strategy, multi-factor authentication (MFA) strengthens security by calling for more than a username and password, substantially lessening the chance of cyber attack. The user-provided authentication information for third-party verification is not related to extrinsic hardware or software. At the time of registration, users save a pre-defined set of functions or themes on their devices, which they provide after they pass the initial verification process. Service providers can use different methods to enable third-party authentication. Role-Based Credential Single Sign-On (RC-SSO) is a quick and secure authentication system that allows first responders and their remote crews to have seamless access. Through the use of role-based certifications, it makes sure that only approved users are able to connect to critical mobile communication networks, providing increased security and operational effectiveness in the event of an emergency.

1.1 Problem Statement

- 1 Cloud application development needs secure and reliable user verification to ensure identity management. Authentication ensures only authorized user access
- 2 Simple online services with single-tier authentication can simply adopt this identity management approach. However, single-tier authentication is insufficient to safeguard cloud services since, in order to breach this authentication method, the hacker must guess the password in some fashion, this can be carried through using force of nature or insiders' assaults.
- 3 Many security challenges arise with cloud infrastructure, causing a major hindrance to the development of On-demand computing in the IT industry.
- 4 A research project is now underway to find solutions to security concerns in the cloud. Security as a Service (SaaS) is a special type of centralized and unified cloud-based security solution.
- 5 This approach is still in the works, but it aims to give centralized security to cloud users so that they may feel completely secure about the security of their data in the cloud.

1.2 Goal

The major goal of this survey is to instigate a safe authentication technique for usage in a virtual environment that can identify a user and offer the necessary services to the proper individual.

1. Create a secure cloud authentication model that recognizes a registered service consumer, produces the required services, and show it on the user's cloud interface.
2. Change the proposed access verification method that facilitates seamless sign-on access to authorized platforms, in which the customer only needs to have submit their credentials once in exchange for access to a certain service
3. Create and test a prototype of the required result confirms in order to assess privacy and frameworks, as well as compare it to the current model.

The primary purpose of this study, as stated in Section I, state art methods discussed in Section II. The proposed three-tier authentication technique, as well as Role-Based Credential Single Sign-On (RC-SSO), are explained in Section III (RC-SSO). Section IV displays the implementation details and results for evaluating security and comparing the proposed authentication model to the existing authentication technique with various comparison criteria.

2. LITERATURE SURVEY

Real-time systems are soft, where a large amount of data processing is equally important for contextual awareness, distributed computer systems can hire another layer of data flow, and this study examines how useful those systems are. [1] Along with the general application layout and context or current network layer, the proposed article raises the middle layer between user structures and details. The proposed research also shows how to create this art and how it can be used as a standard model of construction. [2] The project employs JSON-RPC as a communication platform to construct an authentication system and system authentication in a multi-tier telemedicine system. The secure loading of the app upload is studied in this research. Test results confirm that the utilization of JSON-RPC by the multi-tier telemedicine system in medical device authentication has yielded a secure system with a stable loading mechanism. [3] In a multi-level system, the proposed framework aims to develop an entirely integrated modeling function that explores the space of a specific data document. The Request Time and the Central Response Time are calculated utilizing the RDF segregation model across the architecture. The other function is utilized by default in the proposed method, which helps predict request response time. [4] It utilized the structured technology-to-environment (TOE) framework (HOT-fit). Compliance

was then determined via the Analytical Hierarchy Process (AHP) method. The findings of the study thus have important theoretical and managerial implications for paper and paper industry managers, and the manner in which they can promote the sustainability of a multi-level supply chain to enhance competitiveness.

A lightweight and accurate method of predicting failure and finding similar errors in distributed systems is presented in this study. [5] PreMiSE employs a fusion of anomaly-based and algorithm-based algorithms to detect multi-level failures affecting indicators of progress with high accuracy and inferior level of false positives. PreMiSE can actually predict and identify events that may fail with higher and higher accuracy, according to test results obtained from the Cloud-based IP Multimedia Subsystem. [6] This is the first comprehensive assessment of the safety of all approved single vehicle handling applications offered by major European automobile manufacturers operating in Europe. These findings indicate a variety of problems, including the widespread usage of crucial permissions and API calls that might compromise privacy in the execution of CWE and CVE vulnerabilities, the overuse of third-party trackers in some circumstances, and the execution of other third-party-related libraries. Errors linked to use. [7] In three mobile-based health care systems equipped with wearable devices, a new anonymous anonymity system has been developed. The effectiveness of our method has been tested in detail, and its effectiveness is compared with other similar strategies. Our approach beats the existing methods and delivers comprehensive and integrated authentication services.

Multiple authentication strategies have been developed to limit the limitations of a single login process. Verification systems for state-of-the-art technology delivered between 2011 and 2018, their shortcomings and security difficulties, and finally their natural computer solutions. [8] Comparison of available multitier verification strategies is performed in three ways: security level, implementation cost, and usability. Multitier authentication strategies are divided into groups based on aspects of the verification process they face. [9] Improved the growth of one-team and two-level authentication schemes consisting of three layers of web-based banking authentication, including PIN, one-time password (OTP), email notification, and click-through password. Enemy access to unauthorized banking services is hampered by a multi-stage authentication system. Because opponents were unable to violate three categories of authenticity, the system received high accuracy when tested. [10] The hybrid block chain used is used to provide a node openable system. The hybrid block chain approach is intended to improve the compatibility of blockchain and IoT environments. The process of selecting a proxy node is then designed to create a connection between a

blockchain and standard IoT node by checking the amount of confidence between nodes. The model node authorization process and the process of selecting proxy nodes, based on an advanced blockchain, establishes secure inter-network connections. Safety and performance testing reveals safety and efficiency.

It is suggested that you perform an organized survey of current developments in distant user verification plans. There are security attacks that any security strategy should avoid, as well as security standards that must be met by each security scheme. [11] Nearly 100 past user assurance strategies have been tested and compared in terms of key features, security tools used, and operational features such as calculation costs, communication costs, storage costs, accuracy, FAR and FRR. Investigators can easily identify appropriate attributes, potential items, and describe several security attacks as a result of current guidance in the study of remote user verification schemes. [12] With the construction of two WBAN buildings, a unique and validated power consumption plan and key contracts (SEEM) have been developed. SEEMAKA offers excellent security features and prevents a variety of security attacks with hash reduction and low XOR performance, suitable for limited power sensors. SEEMAKA surpasses other modern systems of verification by further processing, power distribution, and safety features, [13] which is anticipated to improve overall rendering and promote better service delivery based on a variety of planning and design, thus providing superior services and creating many strengths.

A structure supported by mobile edge computing (MEC), consisting of tier nodes, core, edges, and devices, is proposed to meet the ultra-low latency requirements of 5G. The optimal amount of traffic under a fixed volume is calculated using linear reasoning, [14] and the allocated volume is also reduced under a fixed vehicle allocation to satisfy a percentage of the delay. Construction by the MEC could save 20.7 percent of the energy in the construction of two buildings. The proportion of the satisfactory delay is 90%, compared to 50%, an additional 12.2 percent must be provided. [15] The proposed and built-in system uses the Raspberry Pi, powered by Internet of Things (IoT) and integrated with several sensors such as DS18B20, ADXL345, ADC1015, and heart rate sensor. With an improved view of patient data, the proposed system creates a real-time graph of data such as body temperature, heart rate, and body position, compiled by GPIO. system analyses the different types of sample groups and provides details on probability analysis.

A detailed strategy for allocating network resources for three-thirds networks is explained, based on exchange simulations. [16] High outflows with minimal delays can be obtained using the proposed resource allocation method. [17] The performance implications

and benefits of utilising QoE to transfer a function from the cloud to higher-level nodes in a video distribution line. Discussion of service migration to minimise congestion on the main network, as well as the trend of service migration across multi-tier nodes, as well as prospective research issues and possibilities. In a growing consumer wireless environment everywhere, an intelligent recommendation system is used to acquire and promote to users "advanced" mobile services (UCWW). [18] A Data Processing Framework (DPF) leveraging Lambda's three-tier architecture is introduced within the cloud environment. To ensure high efficiency and minimal latency, two decentralized "publish-subscribe" modules powered by Kafka were developed for handling data processing, registration, and message storage. The effectiveness of the Kafka-Storm-Kafka DPF component is largely determined by the configuration of cloud-hosted Kafka Brokers and Storm Supervisors.

Our goal is to achieve a high level of security without compromising user usage. Some authors have recommended strengthening security by installing multiple components, but this is not the best method because it creates usability issues and increases the complexity and cost. [19] Compared to previous authentication strategies, graphic passwords offer users greater comfort and security at a lower cost. Verification systems based on predetermined patterns and behaviours are very expensive for everyday internet users, but online banking assurance strategies should be very secure. [20] A weakness in the S-Mbank technique is the use of a single-time password given to a user's mobile phone through short messaging service (SMS). To improve computer performance, use a text scheme. As a solution to the shoulder attack, authentication from the paired text is also recommended with the login process. A novel safe and efficient mobile user authentication procedure for On-demand computing has been created using cryptographic hashes, bitwise XOR, and weird extraction algorithms. [21] The proposed process has a much lower cost of computation compared to existing systems because it does not use any limited resources. The proposed method is free from registration centre throughout the verification process, resulting in lower communication costs compared to other similar schemes.

A medical professional may access patient data stored in the cloud from anywhere on the planet. Thanks to an efficient user verification process, only authentic users have access to data and services. For remote patient monitoring, a user authentication technique that is both secure and efficient. The technique proposed is dependable, straightforward, and resistant to typical security risks. [22] The scheme's calculating head is small. The suggested system's security is ensured by an official verification utilising the AVISPA tool. FogHA is an anonymous fog authentication process that helps verify both identities and securely

establishing shared secret keys between nearby fog locations and mobile devices. [23] FogHA has high rendering performance because it uses only the first lightweight cryptographic material and avoids duplicate verification messages with the help of fog. A unique hybrid process that verifies user authentication in the system while also validating whether the user has progressed the biometric system as authentic or untrue. [24] A similar palm-to-face process is performed, and the system allows the user to log in according to the combined evidence. The impactness of the proposed method in executing effective and reliable authentication, overcoming traditional validation restrictions and fraud practices, is confirmed by test results across all benchmark datasets. [25] At WBAN, a number of security strategies and solutions, as well as authentication schemes, were summarized and discussed. Unlike previous research that looked at safety and authenticity on the WBAN in an interesting way to reach key areas in research topic, this study has taken a whole approach to safety with validation on the WBAN. A comprehensive description of the security measures on WBANs is provided, as well as a comprehensive survey of security requirements, security attacks, adversaries and their attempt strategies, and current solutions.

To improve security, this system uses a three-distinct architecture with two polynomial collections that include sensor nodes, mobile sinks, and certain access points that can act as sensor nodes. [26]. The observation time, dissemination loss, latency, false alarm factor, and selection of vehicle are all used to evaluate RVAC performance [27]. For emergency and rescue operations, a revolutionary three-distinct communication security model (MuSE). MuSE prohibit network access to save fighters' clients at the mobile client layer using the weightless standard EAP-PSK and a new TETRA-based Dynamic key Distribution technique (TEDDi) [28]. The UIAP-based weightless technical implementation of Unified login method for multiple applications and key agreement. This paper also explains how to use lightweight SOAP services to build the authentication method on a cloud-based platform. [29]. To provide a satisfactory level of data transfer and time security. Because authentication protocol research is still relatively new, the number of new security protocols is expanding at the same time as new threats emerge, therefore the focus of future research will be on proving their efficacy [30].

3. PROPOSED METHOD

Three-tier authentication (TTA) is an identity verification method that requires a user to give two or more authentication components with the goal of get access to resources such as a programme, an online account, or a VPN. MFA is required for an effective copyright and access control (IAM) policy. MFA needs

one or more authentication stages in addition to a login and passphrase, reducing the likelihood of eminent cyber-attacks. External hardware or software are not required for the user's information to be used for third-party authentication. The user registers a series of function or sequences during registering and sends it after passing the first team verification. Any strategies that the service provider may use to create third-party authentication.

3.1 Three-Tier Authentication

A three-tier authentication process to overcome internal attacks and to provide one-on-one access to registered services by modifying the existing three-tier authentication procedure for cloud services employing RC-SSO is a three-tier authentication paradigm with one additional authorization for the intended user. Three phases of authentication are used in the proposed verification method. The first group validates users using a secret code, the second authorises consumers using pattern matching, and the third category confirms users using a password. The user types the URLs of the cloud providers into his

browser. The cloud service provider's server receives queries from the user's browser. The GUI login is loaded by the cloud platform from the browser window. To complete the initial authentication process, the user inputs their login details into the login GUI.

This login information is transferred to the service provider's server. The user's account and password are verified by the cloud server. The cloud server sends a verification answer to a single client-side scheduled application only if the given details are correct. The viewer receives a verification response from the virtualized server to determine if additional verification is required. The monitor instructs the software to display a design-matching screen, which is a simulation screen in the browser, if the verification answer agrees. OTP serves as the key to the third stage of authentication. OTP is sent to the user's registered email id. The central authority authorizes OTP; if permitted the user completes the authentication stages and is granted access to the Cloud Service Provider.

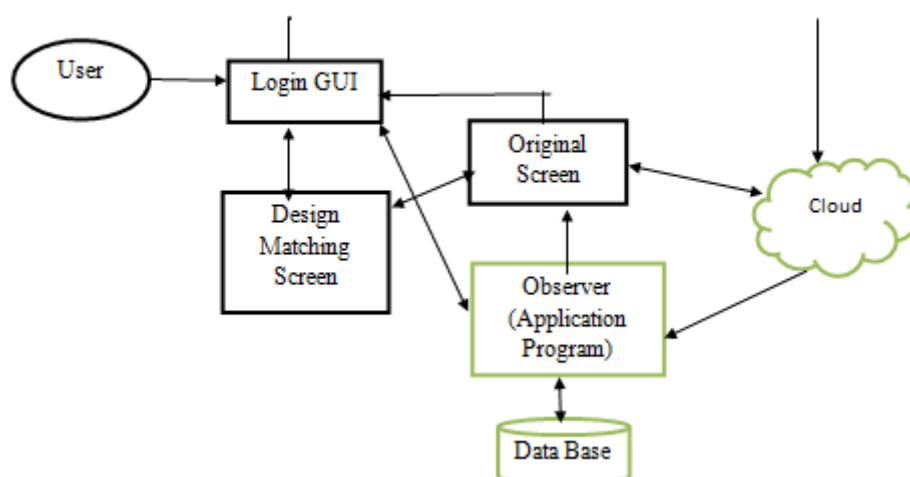


Fig 1. Overall Architecture

The fake screen retrieves user authentication information from the database in order to validate the second phase authentication credentials. The application programme loads the design matching screen in the client's front-end after retrieving the data from the database. The application programmed continuously monitors the user's web browser with the goal of validating the user during the second phase of authentication. The second phase verification credentials are a series of activity or design.

The application or observer is always monitoring these designs and activities. If the observer recognises the right pattern of the user's second phase authentication, it returns to the starting screen of the requested service. The observer loads the original

screen into the user's web browser after beginning the original screen. Once the first screen in the browser is loaded, the cloud server initiates direct connection with the user for future operations in the loaded service.

3.1.1 Authentication Metrics

An authentication metric is a form of user metadata employed for identity proof. TTA is employed to establish who you are, what you possess, and where you acquired the access. The most widely employed three metrics are as follows

- Knowledge metric: It relies on knowledge-based authentication (KBA). In this, the consumers have

secret, and the authentication token is kept on their behalf by the mobile device they use to log in.

2.Identity servers

There are several identification servers in the scheme: $IS(1), IS(2), \dots, IS(n)$. Every identification server verifies the user's information by checking the correctness of the password.

3.Application servers

Application servers, which utilise users are authenticated via identities servers, are the responsibility of mobile service providers. If the authentication is successful, the user can ask the application servers for mobile services. This password-based single-sign-on authentication solution comprises two phases: registration and authentication. Six algorithms for mobile users are Setup, MainKeyGen, Register, RetriSerPsw, Authentication, and RenewShare.

3.2.2 Registration

Phase 1. Registration. System settings are produced during this stage, and smartphone users sign up for identification servers. Three strategies are used in the

registration process. Setups, MainKeyGen, and Register are all included.

3.2.2.1 Setup

The system parameter is received, which is produced and distributed to users and identity servers. The system has been started, the PP system parameter has been set, and PP has been dispersed among all scheme parts. Using the security parameter l , the system parameter PP is calculated. ρ are the maximum number of authentication token requests a user may make in a given time, \emptyset is the maximum number of times a user can fail to authenticate with identity servers, n is the total number of identity servers, and E is a secure symmetric key encryption technique.

3.2.2.2 Main Key Gen

The global variable is used by the technique to share a main restricted key mrk across all analyse servers, with AS_i 's main restricted part mrp_i . MainKeyGen An analyse server AS_i generates its main restricted part mrp_i using the global variable and the decentralized secret image sharing protocol. $GMSK$ and $GMSK_i$ are the matching main primary key and main general part, accordingly. main restricted $mrk = s$, general main key $GMSK = GS, AS_i$ main restricted part $mrp_i = s_i$, and corresponding general main key $GMSK_i = GS_i$.

Algorithm 1. Protocol for distributed secret sharing

Security parameter l , analyse server indexes $\{1, \dots, n\}$, and analyse server index i are all required. Ascertain that all analyse servers share a secret s and the accompanying general key GS ;
 Compute a secret share S_i and the matching general share GS_i , $i = 1, 2, \dots, n, AS_i$.

1. IS_i randomly choose $a_{i,0} \in Z_p^*$ and a polynomial $f_i(x) = a_{i,0} + a_{i,1}x + \dots + a_{i,t-1}x^{t-1}$ over Z_p with degree at most $t-1$ such that $f_i(0) = a_{i,0}$;
2. For $\epsilon = 1, 2, \dots, t-1$, IS_i sends $a_{i,\epsilon}G$ and $a_{i,\epsilon}G$ to all other analyse servers. AS_i sends $f_i(j)$ secretly to AS_j for $j = 1, 2, \dots, n; j \neq i$;
3. Once you have received it, $f_j(i)$ from $AS_j (j \in [1, n], j \neq i)$, AS_i verifies $f_j(i)G = \sum_{y=0}^{t-1} i^y \cdot a_{j,y}G$. If the verify is unsuccessful, AS_i rejects;
4. AS_i computes the secret share $s_i = \sum_{y=1}^n f_j(i)$ the general share $GS_i = s_iG$;
5. AS_i computes general key $GS = \sum_{i=1}^n a_{i,0}G$ securely stores s_i , maintains $\{GS_1, GS_2, \dots, GS_n\}$, and deletes other values.

The secret key $s = \sum_{i=1}^n a_{i,0}$ is delivered to all analyse servers, it is not expressly included in the scheme.

3.2.2.3 Register

This method is run interactively by U and all of the analysis servers. U , a smartphone user, creates an account with the analyze servers.

Step 1: U creates an AD_U user analysis and a psw_U . U human memorable password. $r \in Z_p^*$ is chosen at random by you. $psw_U^* = rH(psw_U)$, is computed, and (AD_U, psw_U^*) is sent to all analysis servers.

Step 2: GS_i examines if AD_U exists in its local storage for $i \in [1, n]$, GS_i , and if it does, IS_i alerts U that the analyse of the user is duplicated Instead, GS_i stores

AD_U and dictates that U is the group's initial member, requiring the analyse server to produce for such a set of users, a server key

Step 3: The distributed secret sharing protocol is used by GS_i to produce the server-side key share.

Step 4: GS_i computes $\sigma_i^* = k_i \cdot psw_U^*$ and sends to U . U check the validity of σ_i^* by checking

$$e(\sigma_i^*, G) = e(psw_U^*, GS_i).$$

After receiving t valid signature U computes

$$w_n = \prod_{1 \leq t \leq t, t \neq n} \frac{l}{l-n}, \tag{1}$$

$$\sigma_u = r^{-1} \sum_{n=1}^t w_n \sigma_n^* \quad (2)$$

Step: 5 U computes a server derived password SP_U as

$$SP_U = F(h(\sigma_u), psw_U).$$

Step 6: For $i = \{1, 2, 3, \dots, n\}$, U computes $SP_i = h(SP_U || i)$ and send SP_i to GS_i .

Step 7: IS_i stores SP_i and starts two counter-attacks $\rho_u = 0$ and $\phi_u = 0$. U deletes $\sigma_u, r, SP_U, SP_i, GS_i$. and securely stores for authenticating U .

Step 8: k_i is used by AS_i to produce signatures for other members of same team to generate new client key shares for the very first user in a separate group, all analyse servers repeat the previous operations.

The analysis providers produce and share a client key k (the associated General key) for U and GK_i does have a client key share k_i with the associated General share GK_i , U prepares an analyse AD_U and a password psw_U , blinds psw_U to acquire psw_U^* , and transmits it to the analysis servers.

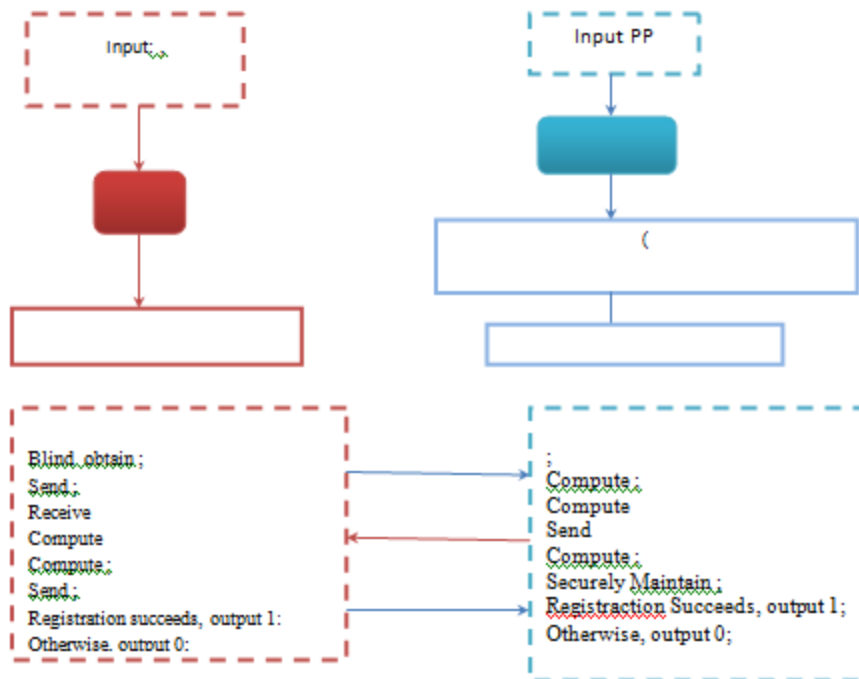


Fig. 3. Overview of Registration

Using k_i to retrieve AS_i signs psw_U and sends it to U . U combines t signatures to get a signature on psw_U under k and evaluates a password obtained from the server sp_U after getting t signatures. Finally, for AS_i , U computes an authentication credential sp_i using sp_U and psw_U . Both mrp and k are created via a distributed secret sharing approach without the use of a trusted dealer, ensuring that mrp and k cannot be extracted by any analyse server and that less accommodating than t analyse servers would not compromise the security. After completing the registration process, a smartphone user just needs to remember her or his password in order to authenticate

3.2.2 Authentication

In the second stage, a smartphone user requests an authentication token from the analysis servers. The sign-on process utilizes the **RetriSerPsw** and **Authentication** algorithms.

3.2.3.1 RetriSerPsw

This method is run interactively by U and all of the analysis servers. U gets σ_U from analysis servers, σ_U is a type of sign psw_U under k and is employed in the computation the password generated from the servers. Analyze servers send you an authentication token share once the authentication is successful. SP_u retrieves the password and generates an authentication token.

Authentication. The technique allows a user to be allowed by analysis server farms and acquire an authorization token and it can be used to access connected services. U computes sp_U and then computes the authentication credentials with σ_U and psw_U . If the credential is legitimate, each identity server examines it and uses the main key sharing to create an authentication token share if the check is successful. From authentication token sharing, you can get a valid authentication σ token called $AutToken_U$. To protect against relay attacks, the random element r_i is employed.

To prevent eavesdropping attempts, the credential encrypts the interaction messages. U seeks services from connected service providers using $AutToken_U$. If the verification succeeds, the service providers can validate $AutToken_U$ utilizing the fundamental attributes of common servers and providing U with the associated servers. The algorithm RenewShare is

employed during the crucial phase of renewal, where each analyse server renews its main restricted portion mrk_i to avoid main restricted key shares from being compromised. The main restricted key mrk would not be modified after RenewShare to ensure that renewal of main restricted portions did not "break down."

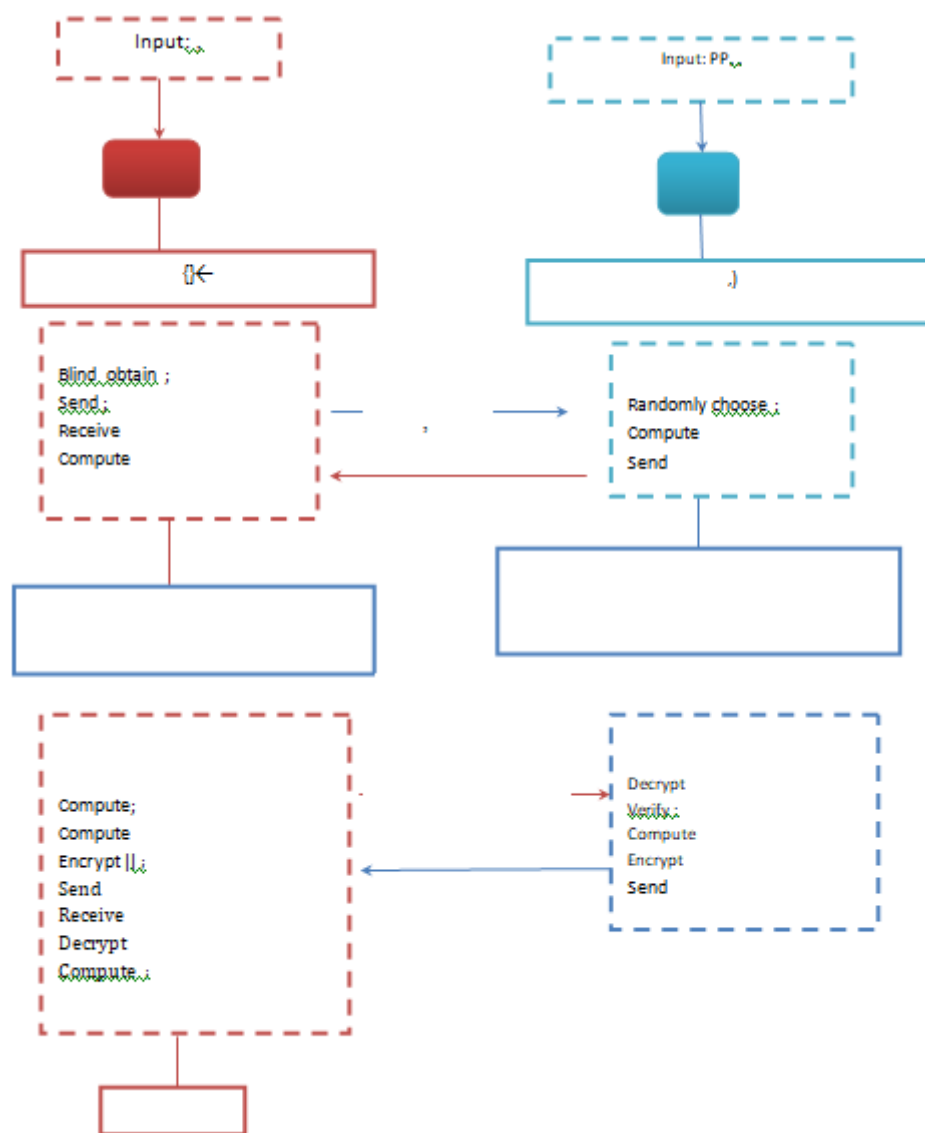


Fig. 4. Authentication Overview

Phase 3: Renewing the key. Each analyse server renews its main restricted portion during this period to prevent share leaking. It re-enforces security and prevents the attacker's effort's ability to continuously breach analyse servers over time. Only once every era is the renewal of main restricted sections performed. **RenewShare.** For each analyse server $AS_i, i = 1, 2, 3, \dots, n$ at the end of each epoch it renews its main restricted part mrk_i .

- AS_i randomly select a polynomial $l_i(x) = b_{i,1}x + b_{i,2}x^2 + \dots + b_{i,t-1}x^{t-1}$ over Z_p with degree at most $t - 1$.
- For $\epsilon = 1, 2, \dots, t - 1, AS_i$ sends $b_{i,\epsilon}P$ to all other analyse server. AS_i sends $l_i(j) \bmod p$ secretly to AS_j for $j = 1, 2, \dots, n; j \neq i$.
- After receiving $l_j(i)$, AS_i checks

$$l_j(i)G = \sum_{y=1}^{t-1} i^y b_{jy} G. \tag{3}$$

It aborts if the checking fails. AS_i generates a new main restricted key share mrk'_i as follows:

$$mrk'_i = mrk_i + \sum_{j=1}^n l_j(i). \quad (4)$$

- The corresponding General main restricted part is $GMSK'_i = mrk'_i G$. AS_i deletes $l_i(x)$, $b_{i,\epsilon}$, $l_i(j)$, and mrk_i .
- Finally, AS_i resets ρ_U and \emptyset_U . A new epoch begins.

Once all the server-derived password candidates are obtained, an attacker can carry out offline DGA to retrieve the target password. Such an attack is called online DGA. In order to prevent such attacks, analysis servers limit the number of queries that one user can make per epoch on login and authentication token generation servers. The users are grouped according to the time of registration, with a specific set being given client keys, and varying consumers being accorded different server-side keys.

3.3 Communication Procedure Of Rc-Sso

The RC-SSO communication technology is used to communicate amongst different entities. An emergency client or entity can use the RC-SSO solution to gain immediate access to the services of multiple entities.

The SSL/TLS communication process is invoked between organizations whenever a client or company requests direct access to information. In order to confirm the validity of contact points, the client and server send their X.509-based certificates for processing. The pre-existing function of the organization is incorporated directly as extra information in X.509 client extensions, minimizing communication operations (messages 1, 2, 3, and 4). This data is then utilized for authorization. Once the integrated approach is authenticated, the client requests information from the web server. The server checks the client's role since the client has presented their certificate and decides the data that can be exchanged according to its policy (messages 5, 6, and 7).

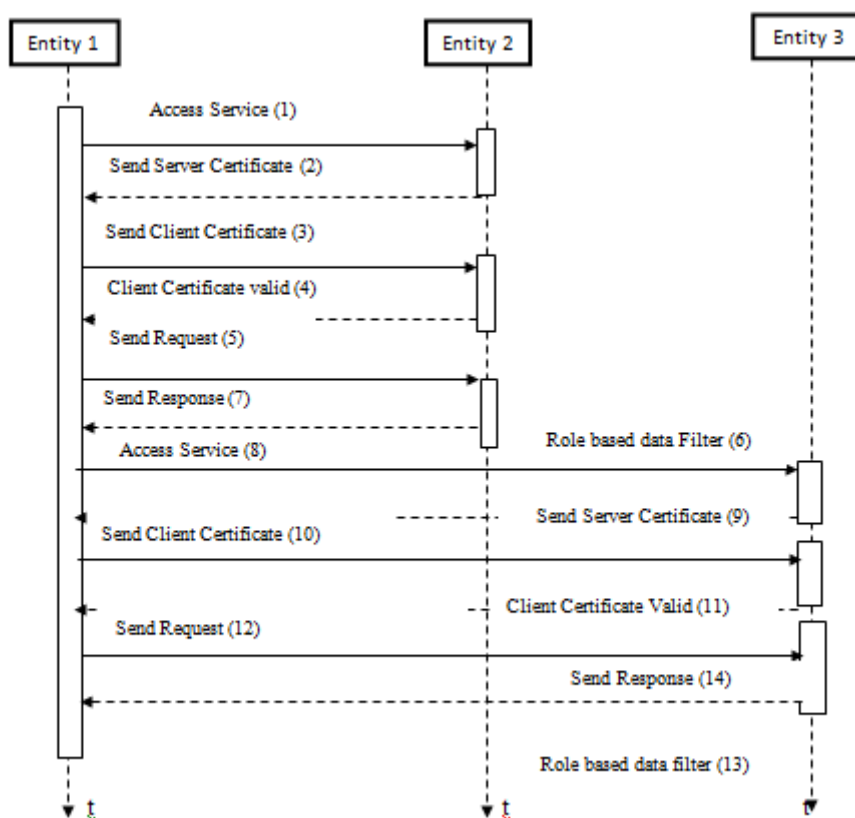


Fig. 5. Procedure for RC-SSO Communication

A reputable Certificate Authority issues the certificates (CA). The German Federal Office for Information Security (Bundesamt für Information's sicherheit) could be a potential CA for disaster and crisis relief teams. Especially compared to other CAs like VeriSign, which manages a wide range of network

equipment, RC-SSO certificates need less administrative effort. It is a reality that which organizations are involved in a disaster relief effort, and knowledge is essential for a successful rescue operation.

4. EXPERIMENTAL RESULTS

Our one-way access role-integrated three-tier authentication certificate is applied to link registered services with Google Co-information conversion. Our procedure employs Google Data Store, a database system hosted by Google on GAE, for cloud app

development. An actual test bed has been developed to measure the performance degradation between unsafe connections and normal SSL/TLS connections among a single mobile client.

Table 1 depicts the limits of various authentication techniques when applying the previously mentioned security criteria.

Table 1. Comparison of various authentication techniques

Authentication Methodology	Security From an insider threat	The presence of authentication relation	No of Security tiers
Proactive Model-based Architecture	No	Server and client	2
RIA optimization on a two-tier architecture	No	Server and client	2
Authentication model RC-SSO	Yes	Server and client	2
Authentication Scheme with Three tier	Yes	Server and client	3

When illustrated in Figure 6, The amount of system memory required by the user develops in lockstep with the number of users that have registered for the cloud service. The FIDO server must link the public key to the user ID when a client sends a public key to validate a signature. The public key's dependability is crucial because the account can be hijacked because of a felicitated public key. As a result, to detect fabrication during the registration process, a method like hash should be utilised.

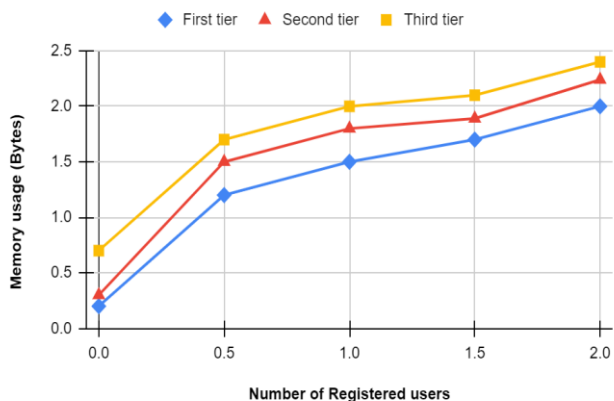


Fig. 6. the amount of memory space required by the user

Figure 7 indicates that utilising SAML instead of RC-SSO increases the average response time by up to 80%. Several new behaviours have emerged as a result of SAML's new communication mechanism. The majority of the time is spent setting up an SSL/TLS-encrypted communication connection. Before going to the IDP for authentication, the client must first establish an SSL/TLS channel with HE. In particular, for attribute retrieval, HE maintains an SSL/TLS communication with IDP.

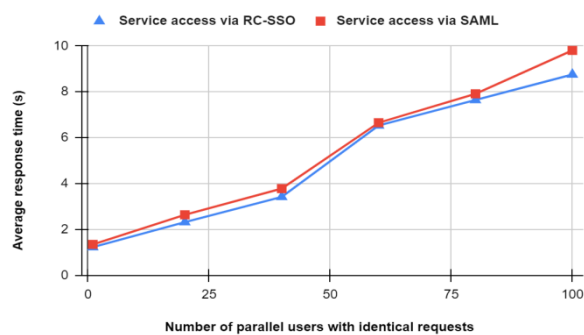


Fig. 7.

Figure 8 depicts the average response time extracted from the simulation model and supported by the test bed. It presents a comparison of the proposed method's average response time and other methods.

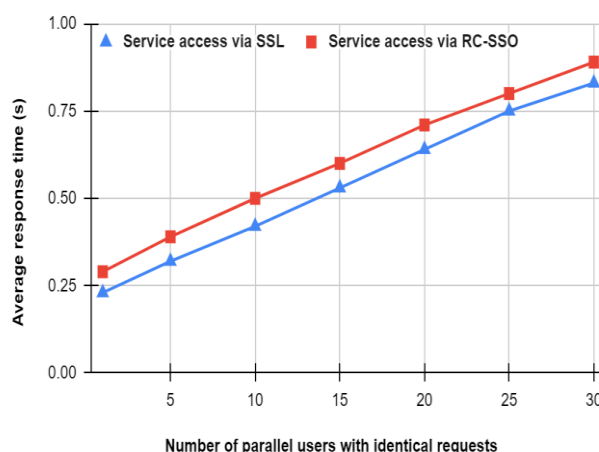


Fig. 8. Average response time comparison of proposed and existing method

Table 2. shows a comparison of the existing and proposed techniques.

Breaking the authentication system's probability of success (p) (let's say $p = 0.1$)	Technique of two-tier authentication	Technique of three-tier authentication (Proposed)
The likelihood of successfully breaching the authentication system, denoted as the probability of success (p), where p equals 0.1	0.01	0.001
Access with a single sign-on (RC)	No	Yes
The total number of authentication factors	One	Two

The existing authentication method and the suggested authentication method are compared and shown in Table 2 with three comparison parameters.

CONCLUSION

This article will try to show the creation of a more advanced and secure authentication system. As technology rapidly progresses, security, in general, as well as the means of authentication, needs to be improved along with it. Experts point out that the possibility of invading a multi-level authentication system diminishes to close to zero when there are a multitude of layers involved in authentication. Security evaluation discloses that the multi-layer method of authentication involves an incredibly minimal chance of getting compromised. The suggested approach, although it consumes much more storage space than existing, more efficient authentication methods, is perfectly adaptable to cloud scenarios where mass storage and scalability are crucial. In terms of storage requirements, while the number of registered users in a cloud application increases, storage for user credentials grows linearly, but processing and retrieval overhead on the cloud server does not change. The suggested authentication method utilizes a secret code received on a smart phone to provide single-sign-on access to cloud services offered by service providers. To gain access to these services, users are required to provide a secret code received on their registered phone number. This process makes the suggested method immune to masquerade attacks.

REFERENCE

- Kumar, Amit; Mozar, Stefan (2021). [Lecture Notes in Electrical Engineering] ICCCE 2020 Volume 698 (Proceedings of the 3rd International Conference on Communications and Cyber Physical Engineering) | doi:10.1007/978-981-15-7961-5
- Setianto, Dwi, Y., Wahyuningrum, & Estri, S. (2021). Multi-Tier Model with JSON-RPC in Telemedicine Devices Authentication and Authorization Protocol. 2021 7th International Conference on Engineering, Applied Sciences and Technology (ICEAST). doi:10.1109/iceast52143.2021.9426308
- Somashekhar, K., & Eswara Reddy, B. (2021). Performance Evaluation of Multi-Tier Application by using the Comprehensive Workload Modelling in the Cloud. 2021 5th International Conference on Computing Methodologies and Communication (ICCMC). doi:10.1109/iccmc51019.2021.9418275
- Feng, B., Hu, X., & Orji, I. J. (2021). Multi-tier supply chain sustainability in the pulp and paper industry: a framework and evaluation methodology. *International Journal of Production Research*, 1-27. doi:10.1080/00207543.2021.1890260
- Mariani, Leonardo, Mauro Pezzè, Oliviero Riganelli, and Rui Xin. "Predicting failures in multi-tier distributed systems." *Journal of Systems and Software* 161 (2020): 110464. doi: 10.1016/j.jss.2019.110464.
- Chatzoglou, E., Kambourakis, G., & Kouliaridis, V. (2021). A Multi-Tier Security Analysis of Official Car Management Apps for Android. *Future Internet*, 13(3), 58. doi:10.3390/fi13030058
- Li, Xiong, Maged Hamada Ibrahim, Saru Kumari, and Rahul Kumar. "Secure and efficient anonymous authentication scheme for three-tier mobile healthcare systems with wearable sensors." *Telecommunication Systems* 67, no. 2 (2018): 323-348.
- Manzoor, Awais, Munam Ali Shah, Hasan Ali Khattak, Ikram Ud Din, and Muhammad Khurram Khan. "Multi-tier authentication schemes for fog computing: Architecture, security perspective, and challenges." *International Journal of Communication Systems* (2019): e4033.
- Soyemi, Jumoke, and Mudasiru Hamed. "Fraud Detection System using Multi-tiered Authentication Scheme." (2020): 1-10.
- Zhang, Shiqiang, Yang Cao, Zhenhu Ning, Fei Xue, Dongzhi Cao, and Yongli Yang. "A heterogeneous IOT node authentication scheme based on hybrid blockchain and trust value." *KSII Transactions on Internet and Information Systems (TIIS)* 14, no. 9 (2020): 3615-3638.
- Rajasekar, Vani, J. Premalatha, K. Sathya, and Muzafer Saračević. "Secure remote user authentication scheme on health care, IoT and cloud applications: A multilayer systematic survey." *Acta Polytechnica Hungarica* 18, no. 3 (2021): 87-106.
- Narwal, Bhawna, and Amar Kumar Mohapatra. "SEEMAKA: Secured energy-efficient mutual authentication and key agreement scheme for wireless body area networks." *Wireless Personal Communications* 113, no. 4 (2020): 1985-2008.
- Li, Xing, He Jianmin, Bingjie Hou, and Peiyang Zhang. "Exploring the innovation modes and evolution of the cloud-based service using the activity theory on the basis of big data." *Cluster Computing* 21, no. 1 (2018): 907-922.
- Lin, Ying-Dar, Yuan-Cheng Lai, Jian-Xun Huang, and Hsu-Tung Chien. "Three-tier capacity and traffic allocation for core, edges, and devices for mobile edge

- computing." *IEEE Transactions on Network and Service Management* 15, no. 3 (2018): 923-933
15. Kamal, Neel, and Prasun Ghosal. "Three tier architecture for iot driven health monitoring system using raspberry pi." In *2018 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS)*, pp. 167-170. IEEE, 2018.
 16. Shahzadi, Romana, Ambreen Niaz, Mudassar Ali, Muhammad Naeem, Joel JPC Rodrigues, Farhan Qamar, and Syed Muhammad Anwar. "Three tier fog networks: Enabling IoT/5G for latency sensitive applications." *China Communications* 16, no. 3 (2019): 1-11.
 17. Rosário, Denis, Matias Schimuneck, João Camargo, Jéferson Nobre, Cristiano Both, Juergen Rochol, and Mario Gerla. "Service migration from cloud to multi-tier fog nodes for multimedia dissemination with QoE support." *Sensors* 18, no. 2 (2018): 329.
 18. Ganchev, Ivan, Zhanlin Ji, Máirtín O'Droma, and Li Zhao. "Smart recommendation of mobile services to consumers." *IEEE Transactions on Consumer Electronics* 63, no. 4 (2017): 499-508.
 19. Manzoor, Awais, Abdul Wahid, Munam Ali Shah, Adnan Akhunzada, and Faisal Fayyaz Qureshi. "Secure login using multi-tier authentication schemes in fog computing." *EAI Endorsed Transactions on Internet of Things* 3, no. 11 (2018).
 20. Putra, Dea Saka Kurnia, Mohamad Ali Sadikin, and Susila Windarta. "S-Mbank: Secure mobile banking authentication scheme using signcryption, pair-based text authentication, and contactless smart card." In *2017 15th international conference on quality in research (QIR): international symposium on electrical and computer engineering*, pp. 230-234. IEEE, 2017.
 21. Roy, Sandip, Santanu Chatterjee, Ashok Kumar Das, Samiran Chattopadhyay, Neeraj Kumar, and Athanasios V. Vasilakos. "On the design of provably secure lightweight remote user authentication scheme for mobile cloud computing services." *IEEE Access* 5 (2017): 25808-25825.
 22. Sharma, Geeta, and Sheetal Kalra. "A lightweight user authentication scheme for cloud-IoT based healthcare services." *Iranian Journal of Science and Technology, Transactions of Electrical Engineering* 43, no. 1 (2019): 619-636.
 23. Guo, Yimin, and Yajun Guo. "FogHA: An efficient handover authentication for mobile devices in fog computing." *Computers & Security* (2021): 102358.
 24. Sajjad, Muhammad, Salman Khan, Tanveer Hussain, Khan Muhammad, Arun Kumar Sangaiah, Aniello Castiglione, Christian Esposito, and Sung Wook Baik. "CNN-based anti-spoofing two-tier multi-factor authentication system." *Pattern Recognition Letters* 126 (2019): 123-131.
 25. Narwal, Bhawna, and Amar Kumar Mohapatra. "A Survey on security and authentication in Wireless Body Area Networks." *Journal of Systems Architecture* 113 (2021): 101883.
 26. Agrawal, Chanchal G., and J. B. Kulkarni. "Enhancing the security in WSN using three tier security architecture." *International Journal of Innovative Research in Information Security (IJIRIS)* 1 (2014): 40-47.
 27. Tolba, Amr, and Ayman Altameem. "A three-tier architecture for securing IoV communications using vehicular dependencies." *IEEE Access* 7 (2019): 61331-61341.
 28. Sbeiti, Mohamad, Thang Tran, Sebastian Subik, Andreas Wolff, and Christian Wietfeld. "MuSE: novel efficient multi-tier communication security model for emergency and rescue operations." In *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, pp. 929-934. IEEE, 2011.
 29. Anand, Darpan, Vineeta Khemchandani, Munish Sabharawal, Omar Cheikhrouhou, and Ouissem Ben Fredj. "Lightweight Technical Implementation of Single Sign-On Authentication and Key Agreement Mechanism for Multiserver Architecture-Based Systems." *Security and Communication Networks* 2021 (2021).
 30. Mandal, Sanjeev Kumar, and A. R. Deepti. "A General Approach of Authentication Scheme and its Comparative Study." *International Journal of Computer (IJC)* 26, no. 1 (2017): 15-22.