I. J. Computer Network and Information Security, 2013, 1, 65-78
Published Online January 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.01.08

Blactr: A Technique to Revoke the Misbehaving Users with TTP

[1]H.Jayasree, [2]Dr. A. Damodaram,
[1]Assoc. Prof, Dept. of IT, ATRI, Uppal, Hyderabad.
[2]Prof. of CSE Dept & Director – Academic Audit Cell, JNTUH, Hyderabad.
[1]jayahsree@yahoo.com , [2]damodarama@rediff.com

Abstract **—** Anonymous credential systems permit the users to authenticate themselves in a privacy-preserving way. An anonymous credential system is of major practical relevance because it is the best means of providing privacy for users. In this paper, we propose a technique known as Blacklistable Anonymous Credentials with Trust Reputation (BLACTR) for revoking misbehaving users with Trusted Third Party (TTP). The technique uses both Certifying Authority (CA) review as well as other user reviews in order to blacklist a user making use of the fuzzy and rule matched to check if the person is to be blacklisted or not. The proposed technique performed well when compared to BLAC and BLACR.

Index Terms **—** Anonymous Credential, Trusted Third Party, Certifying Authority, User Review, , Fuzzy Logic

I. INTRODUCTION

Internet is making information easily accessible to people. More and more people are sharing information over internet for number of purposes. Protecting the privacy of individuals becomes an important task. There is need of such type of applications that gives users liberty over the amount of personal information they have to share [1].Anonymous credential system is a credential scheme in which a user can obtain, delegate, and demonstrate possession of credentials chains without revealing any additional information about themselves [2].For example in a general credential system a user John can receive credentials from his organization for using some resources ,and at certain instant of time he can prove to the organization that he has been given appropriate credentials. In anonymous credential scheme he can do same thing without revealing anything else about his personal identity.

Anonymous credentials are used as a way to prevent disclosure of too much information about a user during the authentication process. There are some basic properties that every anonymous system should follow .These properties are: a) It should be possible for user to selectively disclose attributes. b) An anonymous credential system must be hard to forge. c) A user transfer must be unlinkable and d) An AC must be revocable [3]. The idea for anonymous credential system is derived from blind signature protocols proposed by Chaum. It is the main building block in many applications in which privacy is very important. Stefan Brands improvised on the idea of Chaum by generalising digital credentials with secret-key certification. Brands credentials provide efficient algorithms and privacy in an unconditional commercial security setting. A new technique, multi-show unlinkability adds a new feature to anonymous credential scheme used in constructing privacy enhanced protocols [4].

In this paper we are building anonymous credential scheme using trusted third party services. Trusted third party models are most commonly used in many commercial transactions and cryptographic protocols. They facilitate communication between two parties who trust the third party. On the basis of this trust their interaction is secured. Typically, TTP will be an organization under the control of some regulatory body, whose work is to provide security services, on a commercial basis, to a number of bodies of different sectors (Telecommunication, Finance, retail sectors etc).TTPs exits in both public and corporate domain. TTPs depends on fundamental requirement that TTP should be trusted by the bodies it serves for certain service. The main advantage of TTP is that two users can interact without establishing individual agreements.

Our proposed technique use both Certifying Authority (CA) review as well as other user reviews in order to blacklist a user making use of the fuzzy in the backend. The proposed technique is split into three modules: Trustee Module, Service Provider Module, and Fuzzy Logic Module. In trustee module, the user submits his/her personal details to CA for obtaining either the anonymous or the normal certificate according to the user need. In service provider module,

the user is taken to the service provider page where the person will be able to edit the data. In both the modules, the user is checked if the person is in the blacklist and if so, the user is denied of any service. The edit can be viewed by the CA and rates the user accordingly. The edit is also rated by other users. In fuzzy logic module the ratings are converted to fuzzy and rule matched to check if the person is to be blacklisted or not.

Contributions of the paper:-

- Inclusion of Trusted Third Party (TTP)
- Including other user review in addition to the CA review
- Use of fuzzy logic

The rest of this paper is organized as follows: Section 2 gives a brief description of the related works and in section 3, brief description of BLAC and BLACR is given. Section 4 discusses the drawbacks of BLAC and BLACR and the need for better system. Section 5 gives the proposed BLACTR and in section 6, the results and discussions are presented. Section 7 gives a brief summary of our work.

II. REVIEW OF ASSOCIATED WORKS

There has been many works in the Anonymous credentials principally in the information storing and retrieval process. In this section, we discuss the some of the works related to it. Jorn Lapon et al. [5] proposed a method for brief idea behind enhancing the exiting theoretical model for knowledge processing to do transformation which provide qualitative approach. For growing information driven society, preserving privacy is essential. To protect the user's privacy Anonymous credentials have a solution. They described their classification and measured their implementations. The complete investigation and practical evaluation of the strategies were presented at last. Liu Xin and XuQiu-liang [6] investigated a methodology which employed the techniques of the Sigma-compiler which was based on the linear assumption for simultaneous zero knowledge argument and a variant of Cramer-Shoup encryption. Only for signal length the new scheme enjoyed the advantages of strengthened security, concurrent join and desirable properties in performance. Furthermore, to improve the exclusive pairing operations of the verifier, a competent batch verification algorithm was also provided.

Othman et al. [7] presented a skeleton called Privacy Enhanced Trusted LBS (PE-TLBS) which provided trust services while protecting the client privacy. They only focused on implementing a basic protocol based on anonymous collaboration that allowed users to attest and authenticate an attribute while keeping their identity hidden under anonymity. The main objective behind the approach was to hierarchically encrypt location information using RSA key pairs known as Endorsement Key (EK) and Attestation Identity Key (AIK), and dispense the appropriate keys only to Trusted Group of clients with the necessary permission. Chi Zhanq et al. [8] proposed a brief synopsis on security system satisfying fundamental security requirements including authentication, non-repudiation, message integrity, and confidentiality for VANETs to accomplish privacy desired by vehicles and traceability required by law enforcement authorities. Moreover, they proposed a privacy-preserving defence technique for network authorities to handle misbehaviour in VANET access, considering the challenge that privacy provides avenue for misbehaviour. The system employed an identity-based cryptosystem where certificates were not needed for authentication. For security goals and efficiency, they showed the fulfilment and feasibility of our system with respect to that.

Barisch et al. [9] prepared a key technology for the Future Internet, tackling troubles like the integration of the network and application layer from an IdM perception as well as the use of electronic identity cards which was the SWIFT project leverages IdM . Also, aspects like the mixture of some user devices, backward compatibility and a new access control infrastructure were required by future IdM solutions. Six security and privacy enablers were considered and all these aspects were made by extending existing IdM solutions which were part of the overall SWIFT structure. These enablers have been partially implemented towards a new IdM architecture. Coles-Kemp et al. [10] discussed a relative performance study of low buoyancy in a service provider's ability to protect their personal information. Earlier, to sponsor a service user's confidence building on-line services were not exclusively designed. So to build confidence in their information practices service users had to depend on off-line techniques. In the epoch of on-line public services delivery, that pattern of privacy protection practice potentially had demoralizing consequences for public service delivery and the ability of the most vulnerable to receive the public service support that they need. The study also indicated the interaction possibilities during social computing as part of the service design were one way to help build service user confidence. This paper concluded with examples of social computing used for that purpose.

Since anonymity can provide users the license to misbehave some variants allow the selective de-anonymizing (linking) of misbehaving users upon a complaint to a trusted third party (TTP). To eliminate the reliance on TTP's, some "threshold-based" techniques like, k-Times Anonymous Authentication (k-TAA) [13, 14] have been presented in the literature. K-TAA cannot be used to punish "too-many misbehaviour's" because it necessarily suffers from degraded privacy after k-authentications. So, existing threshold-based technique like k-TAA was improved by d-strikes out mechanism given in [11] that is based on construction of BLAC [11] to provide more flexible revocation. Furthermore BLAC was improved with reputation score, BLACR [12] that adds a score parameter to each entry in the blacklist representing the severity of the misbehaviour and service providers need the overall score of an authenticating user satisfying a particular threshold. With the intention of research works available in literature we propose a technique to revoke the misbehaving users with TTP. Our proposal more efficient compared to BLAC and BLACR.

III. BRIEF REVIEW OF BLAC AND BLACR

In BLAC (Blacklistable Anonymous Credentials) [11], user inputs credential usk , for which a ticket of the form of B_i^{usk} is generated after the anonymous authentication. The ticket is stored with the service provider (SP) for the respective session. As the ticket is of the form B_i^{usk}, the SP cannot know the user details usk as it is very hard to find the discrete logarithm to find usk from B_i^{usk}. Before the authentication process, the user is cross-checked if the user ticket appears in the blacklist for more than a fixed number of times d . If the condition comes true, the user is blocked access to the webpage and in the other case, the user is granted access where the user will be able to edit the data in the corresponding webpage. The user edit is been reviewed by the certifying authority and if it finds that the edit is not suited or some mischievous activity then the user ticket is been added to the blacklist.

BLACR (Blacklistable Anonymous Credentials with Reputation) [12] is an extension to the BLAC method by adding an extra score parameter. The score indicates the extent of the misbehaviour of the user and in BLACR, apart from looking in the blacklist; the user is also looked for the score which should be above a set threshold. BLACR score can be assigned positive or negativebased on the user behaviour. Here also the user inputs credential usk , for which a ticket of the form of B_i^{usk} is generated after the anonymous authentication which is stored with the service provider (SP) for the respective session. Before the authentication process, the user is cross-checked if the user has more a minimum score required for logging in and if it's found that the score is not achieved, then the user is blacklisted. The score is given for every edit of the user by the certifying authority.

IV. DRAWBACKS OF BLAC AND BLACR AND THE NEED FOR BETTER SYSTEM

In BLAC, the user is blacklisted on the basis of d-strike mechanism and in BLACR an extra score based on the reputation is added to it. In both cases, it does not make use of the trusted third party (TTP) but in our proposed technique, we make use of TTP, so as to make the system more stable and decrease the misuse of the data. With TTP, one submits his/her personal details which are encrypted so as to keep the system anonymous. Adding TTPs, will allow tracing back the blacklist people in case of severe misuse whereas in BLAC and BLACR it is not possible. Another added advantage is the fact that only the review of CA is made use of in the BLAC and BLACR, whereas in our proposed technique we are also taking into consideration of other users review. Here a user can view other persons edit and can rate the edits accordingly. We also add fuzzy logic to combine outputs form both the CA and the other persons so as decide on whether the user has to be included in the blacklist. Here we replace the d strike mechanism in BLAC and BLACR with the fuzzy logic which will have better results. In short we add on the concepts of other user review, trusted third party and fuzzy logic so as to have a better system than BLAC and BLACR.

V. PROPOSED BLACKLISTABLE ANONYMOUS CREDENTIALS WITH TRUST REPUTATION (BLACTR)

This section gives a detailed description of the proposed BLACTR. In essence, unlike BLAC and BLACR, here we blacklist a user based on both the certifying authority and also on the other user reviews. We also make use of TTP and also fuzzy logic in the back end to have a better system. The proposed technique is split into three modules: Trustee Module, Service Provider Module, and Fuzzy Logic Module. The block diagram of BLACTR is given in figure 1.

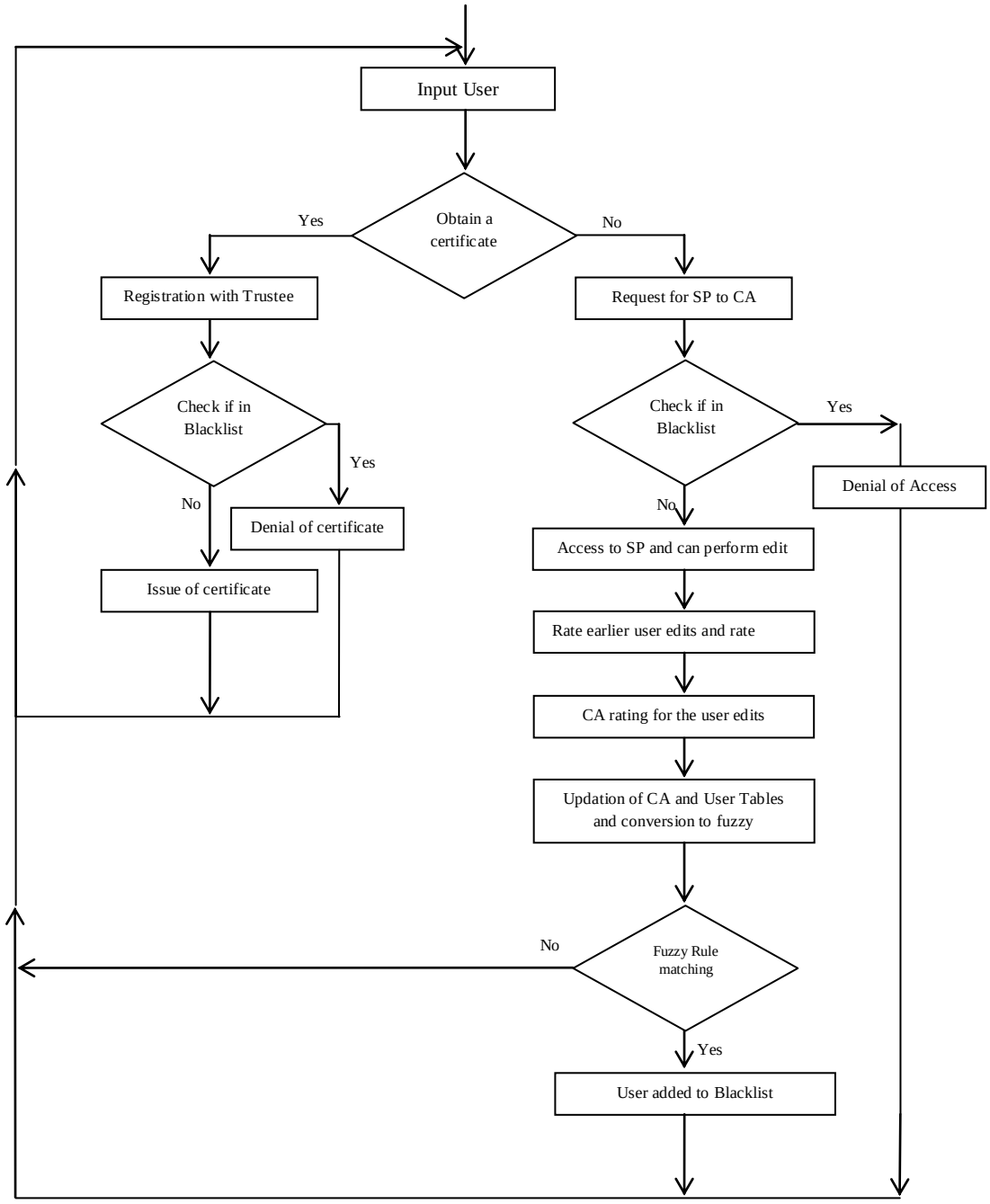

Fig 1: Block diagram of proposed BLACTR

A. Trustee Module

Each of the user in order to attain the certificate registers with the Trusted Third Party (TTP) from the certifying authority. Certifying authority issues either anonymous certificate or the normal certificate according to the user choice. The field that the user has to input consists of name N , age A , passport number P , address R , phone O and mail id M . For a i^{th} user, the fields are represented as $N_i, A_i, P_i, R_i, O_i \; and \; M_i$. In-order to avoid any sybil attack where a user can register even after being black-listed by giving new values in the respective fields, the paper incorporates the passport number field. As any user will have only one unique passport number, the blacklisted user will not be able to log in and will be shown the message that the user is not permitted to log in and that he/she is in the blacklist. The blacklist B has the fields of user ID U , certificate serial number W and passport number S . Therefore for i^{th} user, its passport number P_i is checked with passport number field S in the blacklist B . Suppose there are n number of users in blacklist, so that each of

blacklisted user passport field in blacklist is represented by S_j, $for\ 0 < j \le n$.

$$if \begin{cases} P_i = S_j,\ for\ 0 < j \le n, \\ \quad then\ the\ user\ is\ not\ issued\ certificate \\ \\ P_i \ne S_j,\ for\ all\ 0 < j \le n, \\ \quad then\ the\ user\ is\ issued\ certificate \end{cases}$$

With the user input details, the user can acquire certificate in the normal form or in the anonymous form, if the user is not in the blacklist. The anonymous certificate consists of fields like pseudo name D, public key K, signature of the certifying authority G and certificate serial number E. For a user i, the fields can be represented by $D_i, K_i, G_i\ and\ E_i$. Here, the public key is generated by the RSA algorithm whereas pseudo name and signature is obtained using SHA-256 algorithm. Normal certificate will contain all the details of the user along with public key, signature and certificate serial number. For a user i, the fields are represented as $N_i, A_i, P_i, R_i, O_i M_i, K_i, G_i\ and\ E_i$. Once the certificate is obtained, the user will be able to use this certificate while logging in with the service provider. All the details inputted by the user and the details about the certificate issued is stored in the data base. Figure 2 shows the block diagram for the trustee model.

a) RSA algorithm:

RSA algorithm is used in our paper for public-key generation for the user. RSA cryptography is based on the presumed difficulty of factoring large integers. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. The procedure involved in RSA algorithm for generating public key for the respective user is given below:

- Initially, select two prime numbers a and b randomly preferably having the same length.
- Compute the modulus z for public key given by: $z = a \times b$
- Compute Euler's totient function $\delta(z) = (a-1) \times (b-1)$
- Choose an integer t such that $1 < t < \delta(z)$ and greatest common divisor of t and $\delta(z)$ is 1 and $\delta(z)$ is co-prime. And t is the public key component.
- The public key consists of the modulus z and the public exponent t.
- The user name N is hashed to integer value h.
- With the aid of $z, h\ and\ t$ final public key is generated as $K = h^t (\text{mod}\ z)$

b) SHA 256 algorithm:

The Secure Hash Algorithm is one of cryptographic hash functions published by the National Institute of Standards and Technology (NIST). In our paper, we use SHA 256 to generate the pseudo name and the signature of the Certifying Authority. The methodology involved is explained below.

- The field is first padded with its length in such a way that the result is a multiple of 512 bits long.
- Subsequently, it is parsed into 512-bit message blocks $F^1, F^2, ..., F^n$
- The message blocks are then processed one at a time, beginning with initial hash value H^0, sequentially compute: $H^i = H^{(i-1)} + L_{F^{(i)}}.(H^{(i-i)})$,where L is the SHA-256 compression function, $+$ means word-wise mod 232 addition and H^n is the hash of F.

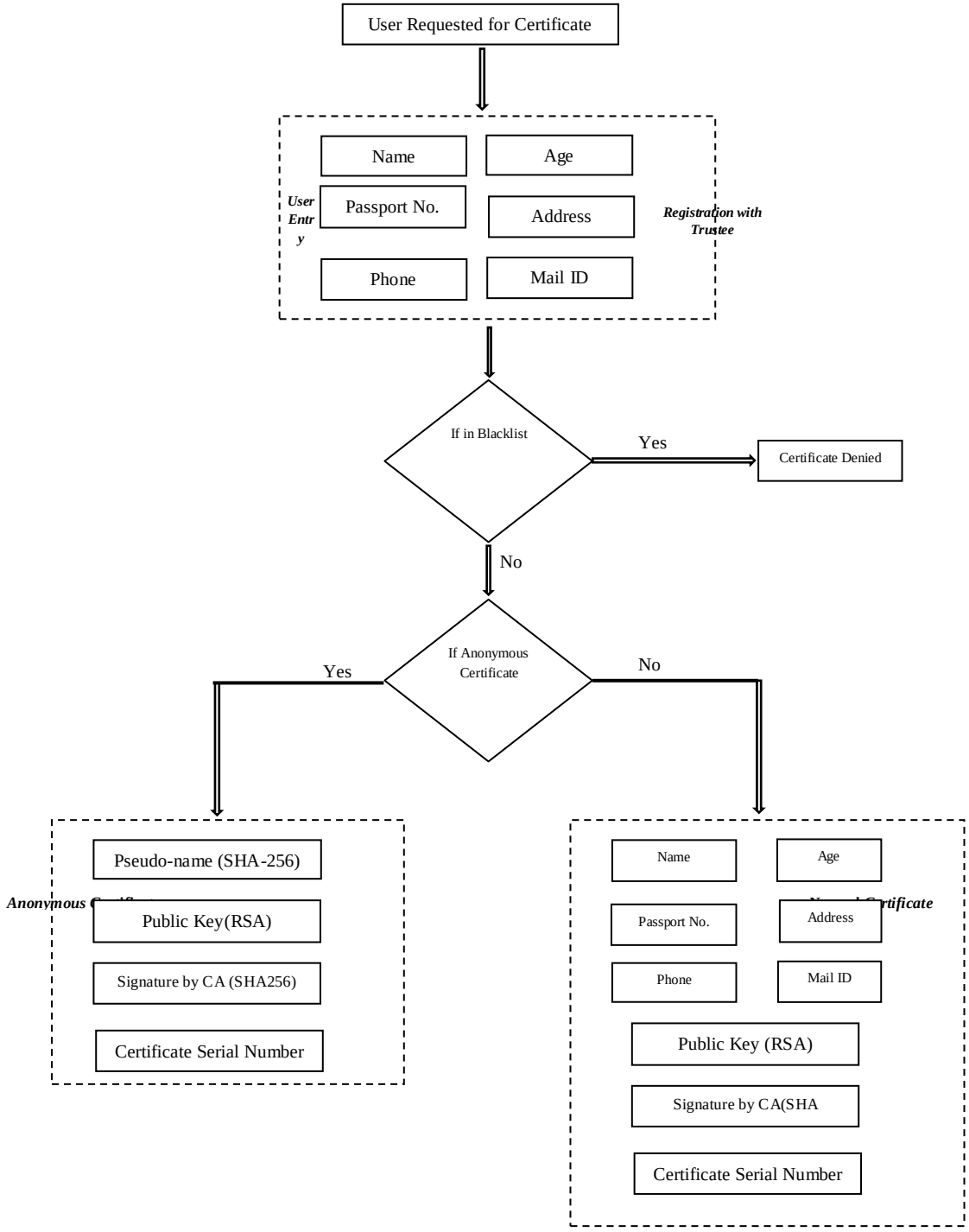

Fig 2: Block diagram of Trustee Module

B. Service Provider Module

The user initially requests certifying authority (CA) for service provider. Upon receiving the request, CA re-directs the user to the corresponding web service page of the service provider requested. Suppose there are m number of service providers represented by $Q = \{q_1, q_2, ..., q_m\}$, the user i requests any one of the service providers q_j, $where\ 0 < j \le m$ and consequently is redirected to the requested q_j by the CA. The user can access the webpage of the service provider in two ways. In the first method, the user will have to enter all the user details along with the username and the password refer. In the other method, the user can access by just providing the certificate details, user name and password. We refer the first method as normal entry method and the second method as the anonymous entry method. The two methods are

briefly described below. Figure 3 shows the service provider block diagram.

a) *Normal Entry*

Here the user inputs his/her personal details in-order to access the service provider. The user has to enter his/her name N^s, age A^s, passport number P^s, address R^s, phone O^s, mail id M^s, user ID X^s and password Y^s. For user i, the fields can be represented by $N_i^s, A_i^s, P_i^s, R_i^s, O_i^s, M_i^s, X_i^s$ *and* Y_i^s. Before granting access, C A checks if the user is in the blacklist by checking the passport number field and the user ID field. If any of the field matches the fields in the blacklist, then the user is not granted access. The blacklist B has the fields of user ID U, certificate serial number W and passport number S. For a user i, it will have the passport number P_i^s and user ID X_i^s which will be checked with S and U fields respectively in the blacklist. Suppose there are n number of users in blacklist, so that each of blacklisted user passport field in blacklist is represented by S_j, *for* $0 < j \le n$ and user id be represented by U_j, *for* $0 < j \le n$

$$if \begin{cases} X_i^s = U_j \ OR \ P_i^s = S_j \ for \ 0 < j \le n, \\ \quad then \ the \ user \ is \ not \ granted \ access \\ X_i^s \ne U_j \ AND \ P_i^s \ne S_j, \ for \ all \ 0 < j \le n, \\ then \ the \ user \ is \ granted \ access \end{cases}$$

b) Anonymous Entry

Here the user can directly access the service provider without the need to enter the full personal details. In this case, the user makes use of the certificate details for the entry. The user needs to enter the pseudo name D, public key K, certificate serial number E, user ID X^s and password Y^s. For user i, the fields can be represented by D_i, K_i, E_i, X_i^S *and* Y_i^s. Before granting access, the CA checks if the user is a blacklisted one and if so, the user is denied access. CA makes use of user ID and certificate serial number to check if the person is blacklisted. For a user i, it will have the certificate serial number E_i and user ID X_i^s which will be checked with W and U fields respectively in the blacklist having n number of users.

$$if \begin{cases} X_i^s = U_j \ OR \ E_i = W_j \ for \ 0 < j \le n, \\ \quad then \ the \ user \ is \ not \ granted \ access \\ X_i^s \ne U_j \ AND \ E_i \ne W_j, \ for \ all \ 0 < j \le n, \\ then \ the \ user \ is \ granted \ access \end{cases}$$

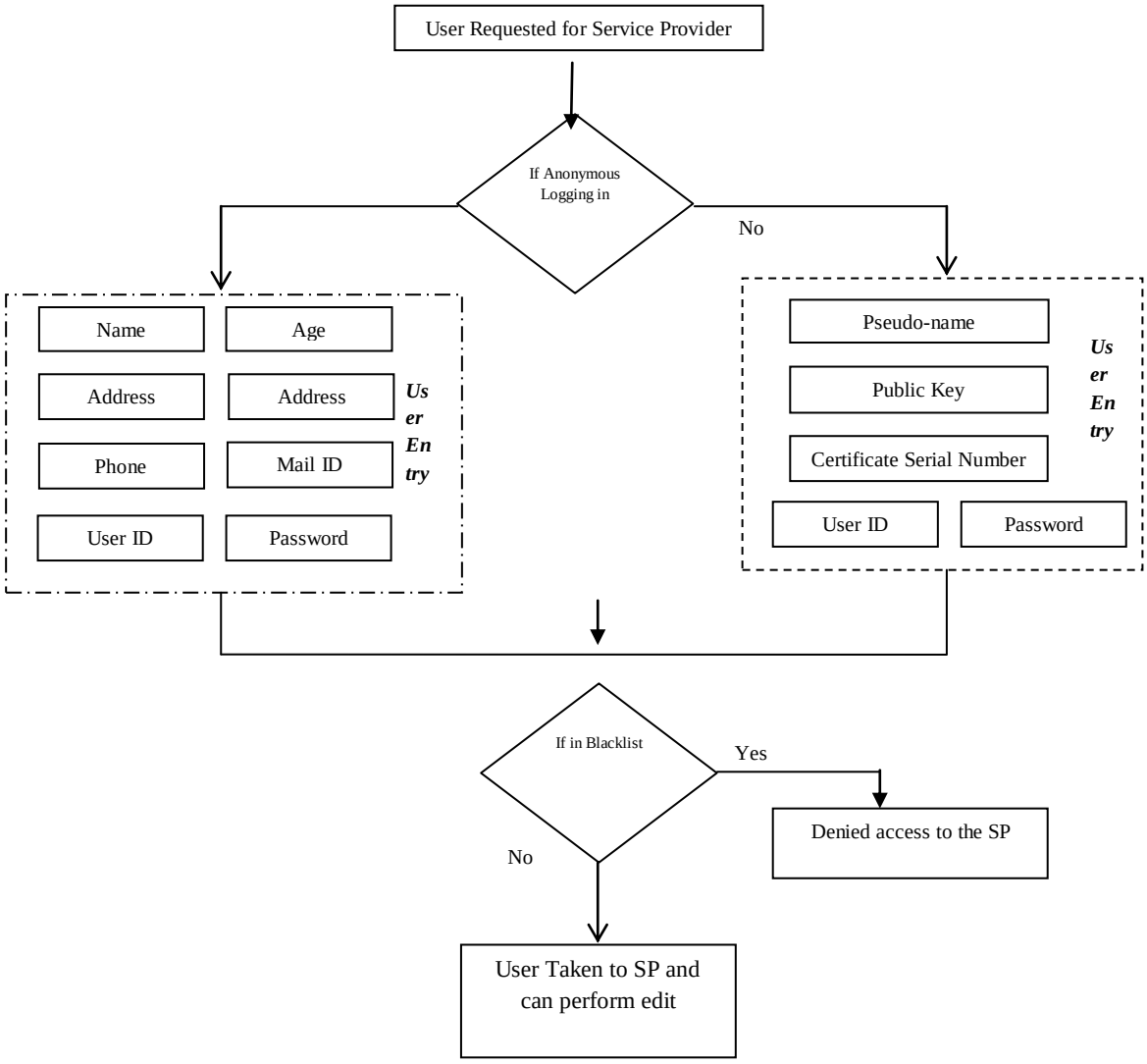

Fig 3: Block diagram of Service Provider Module

C. Fuzzy Logic Module

Once the user logs into the service provider by submitting the details and the CA confirming he is not in the blacklist, the user is taken to the service provider page. In the web page, the user can view and edit the content. The edit the user made is evaluated by the Certifying Authority and rated accordingly. The edit of the user can also be viewed by other users and also can rate the user edit. Both ratings are fuzzified and rule matched to check if the user should be added to the blacklist or not. Figure 4 shows the fuzzy module block diagram.

a) *CA Rating:*

Once the user logs out from the service provider page, the user edit is viewed by the CA and is rated as good or bad respectively. The ratings of the user will be stored in the CA table and each time a user is evaluated, it is added to the respective user rating. In our method, we are converting the CA review into fuzzy values and for any user, the person will have one fuzzy output from the CA table. When the rating given by the CA is good, it is converted to fuzzy value high f_H and when the rating is bad, fuzzy value of low f_L is assigned.

CA Rating	*Fuzzy Value*
Good	f_H
Bad	f_L

If a user has more number of f_H at any time, then the table will output f_H and in other case, table will output f_L for the user. Suppose for the user i edits the service provider page for p number of cases of

which CA rated him as good for q number of times and bad for r number of times. That is, number of f_H values in the CA table is q and number of f_L values in the table is r.

$$For\ user\ i \begin{cases} q > r,\ The\ output\ of\ the, \\ CA\ table\ is\ f_H\ \ for\ user\ i \\ q \le r,\ The\ output\ of\ the, \\ CA\ table\ is\ f_L\ \ for\ user\ i \end{cases}, p = q + r$$

Therefore for any user at any time, the CA table will have either the fuzzy values f_H or f_L.

b) *User Review:*

Unlike BLAC and BLACR, for blacklisting a user we take into account the user reviews apart from the CA rating. The user edit can be viewed by other users and can be rated also. The user review rating is given same importance as the CA rating and other users can rate user edit as Excellent, Good, Bad or Irrelevant. Here also, user ratings are converted to fuzzy values H and L and for any user and there will be one fuzzy value output from the user review table for a user. When the review made by a user is excellent or good, it is converted fuzzy value high f_H and in other cases, it is fuzzy value low f_L.

CA Rating	*Fuzzy Value*
Excellent	f_H
Good	f_H
Bad	f_L
Irrelevant	f_L

For any user, if the number of times f_H appears is more than f_L in user review table, the table outputs fuzzy value f_H and in other case, table will output f_L for the user. Considering the edit of user i and let total number of other users who have reviewed the user edit is y. Of which, u have rated the user as excellent, v as good, w as bad and x as irrelevant. That is, number of f_H values in the CA table is $u+v$ and number of f_L value in the table is $w+x$.

$$For\ user\ i \begin{cases} (u+v) > (w+x), \\ The\ output\ of\ the, \\ user\ table\ is\ f_H\ \ for\ user\ i \\ (u+v) \le (w+x), \\ The\ output\ of\ the, \\ user\ table\ is\ f_L\ \ for\ user\ i \end{cases}, y = u + v + w + x$$

T herefore, the user table output will be either f_H or f_L for the corresponding user.

c) *Fuzzy rule matching*

The fuzzy outputs from both the CA table and user table are combined and rule matched to check if the user should be blacklisted or not. The output for a user i at any time will be either f_H or f_L. When both the table outputs are f_L, the user is added to the blacklist (known as matching case) else in other cases, no action against the user is carried out.

Fuzzy Output from CA table	*Fuzzy output form User table*	*Result*
f_H	f_H	*No action*
f_H	f_L	*No action*
f_L	f_H	*No action*
f_L	f_L	*Blacklisted*

For an user i, let the fuzzy output from the CA table be represented by CA_{fo} and output from the User table be UT_{fo}.

$$For\ user\ i \begin{cases} CA_{Fo} = f_L\ AND\ UT_{Fo} = f_L, \\ User\ is\ added\ to\ blacklist \\ CA_{Fo} = f_H\ OR\ UT_{Fo} = f_H, \\ No\ action\ taken \end{cases}, y = u + v + w + x$$

So, accordingly the user is blacklisted or not based on both the CA rating and User rating.

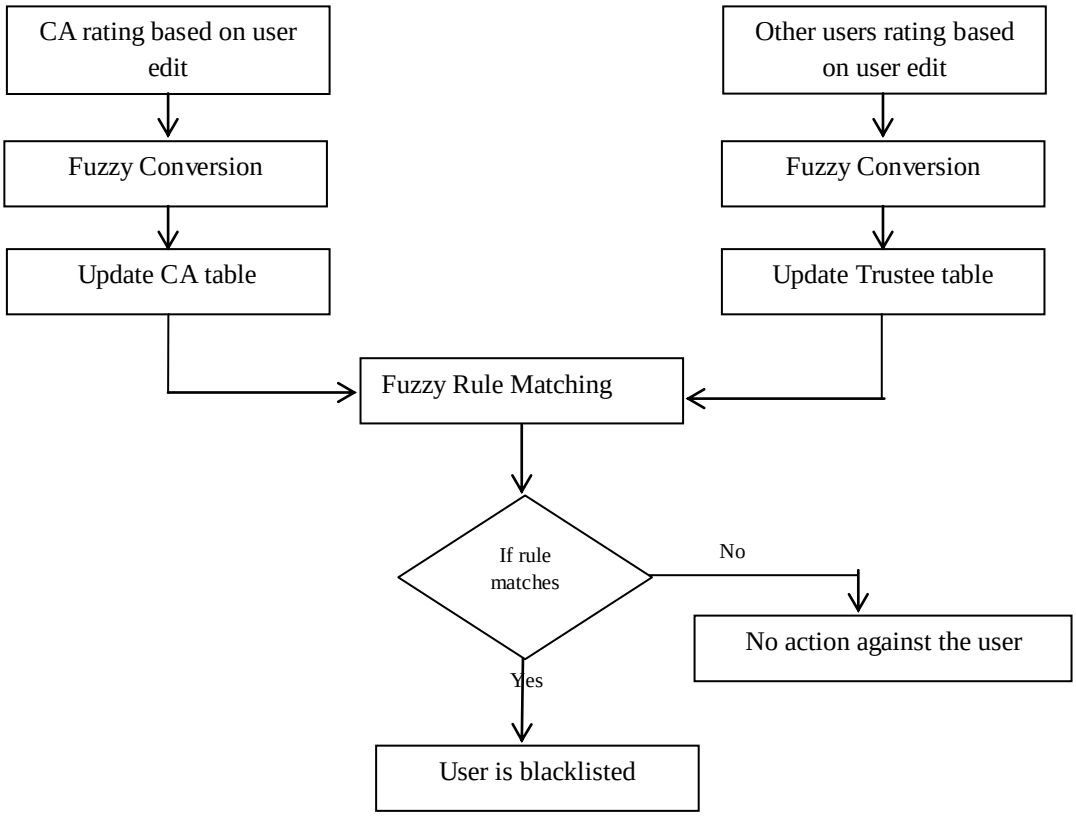

Fig 4: Block diagram of Fuzzy Logic Module

VI RESULTS AND DISCUSSIONS

This section gives the results and discussions of the proposed BLACTR. Section 6.1 gives the experimental setup and section 6.2 gives the screen shots of the proposed BLACTR. Comparative analysis is made with BLAC and BLACR in the section 6.3.

A. *Experimental Set Up:*

The proposed technique is implemented in JAVA SWING. The system on which the method was programmed and developed was having 8 GB RAM with 64 bit operating system having i7 Processor. For the purpose of evaluation, we have taken the details of about 50 users including the user details and the user edits. Every time when a user logs in by giving either user credentials or the certificate, the user edit is made and is reviewed by the certifying authority and other users based on which the user ids blacklisted or not. The total number of edits by the taken 50 users came about 1000. The user edit is also manually reviewed so as to find the efficiency of the techniques.

B. Screen Shots of the Proposed BLACR

This section gives the screen shots of the BLACTR implementation. Figure 5-14 shows different screen shots of the implementation of the proposed BLACTR. Figure 5 gives the home screen having two options either to register with the trustee or directly access the service provider. Figure 6 gives the registration with the trustee giving personal details and the user can ask for anonymous certificate (figure 7) or normal certificate (figure 8).

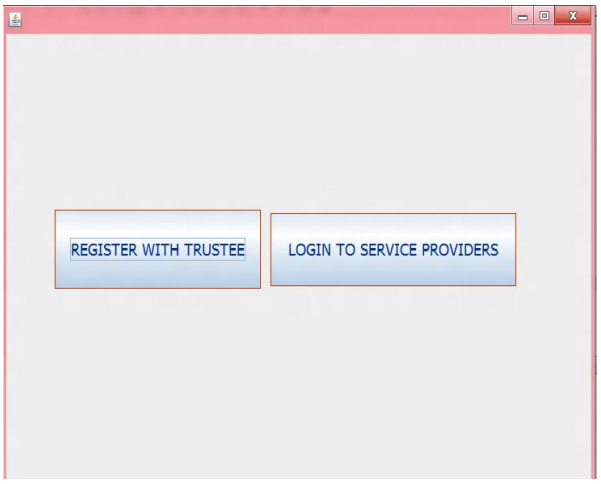

Fig 5: Home page

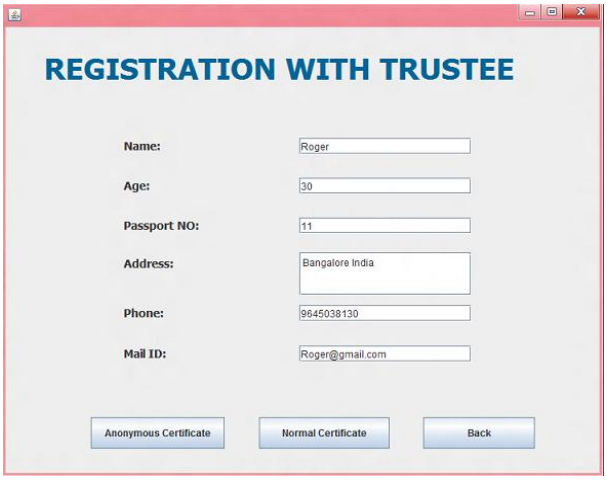

Fig 6: Registration with trustee

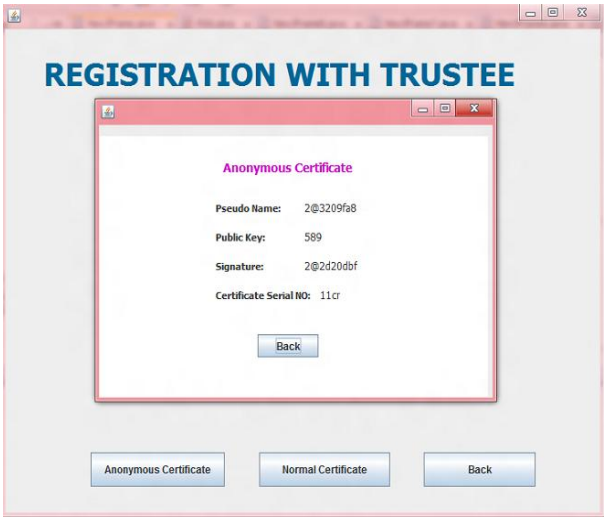

Fig 7: Anonymous Certificate generated by CA

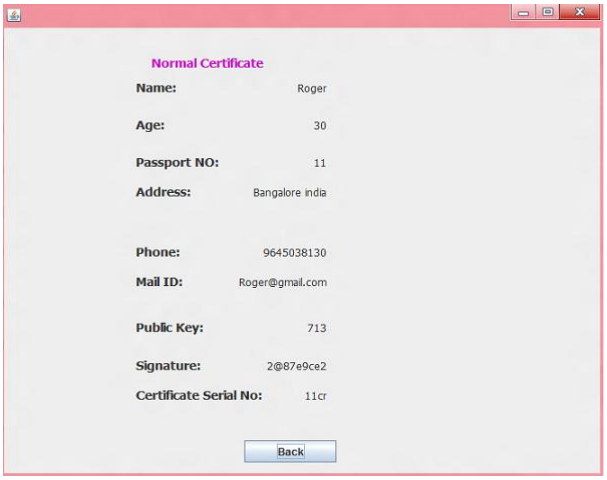

Fig 8: Normal Certificate generated by CA

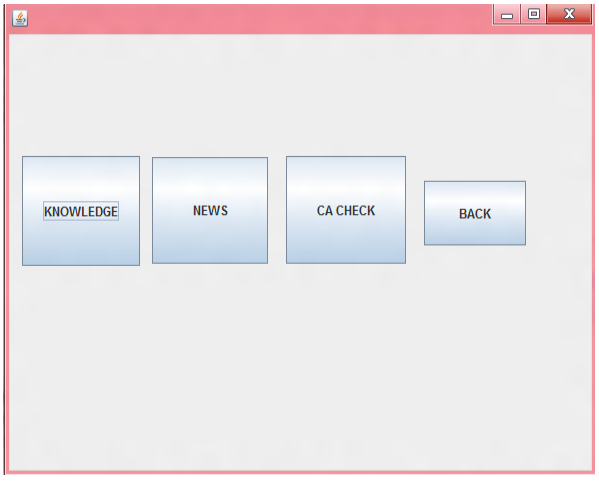

Fig 9: Service Provider Selection Page

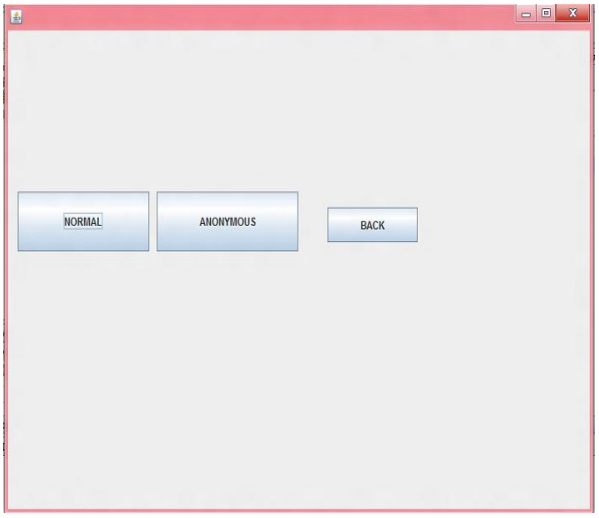

Fig 10: Service Provider Entry Page

Once the user obtains the certificate, he is guided to the service provider selection page (figure 9) of which he can choose his/her option. The user can access the service provider page either by normal or anonymous way (figure 10).

Service provider page entry using anonymous certificate is shown in figure 11 and the page is given in figure 12. The page can be edited and also be modified. The manager review table is shown in figure 13. The blacklisted user message is shown in figure 14.

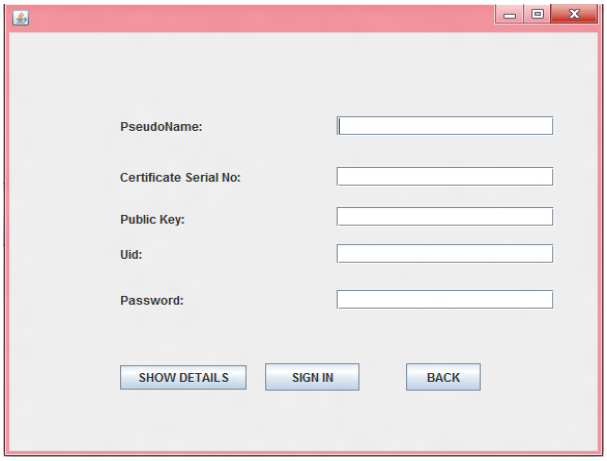

Fig 11: Service Provider Entry using Anonymous Certificate page

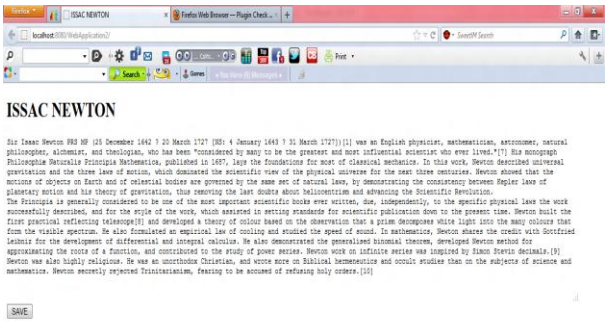

Fig 12: Service Provider Page for Edit

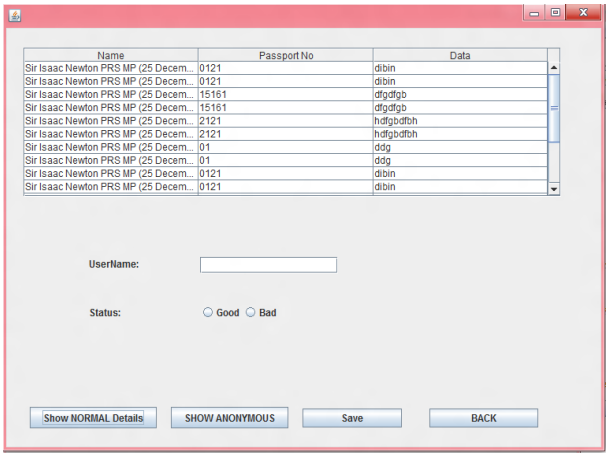

Fig 13 : Review page for manager

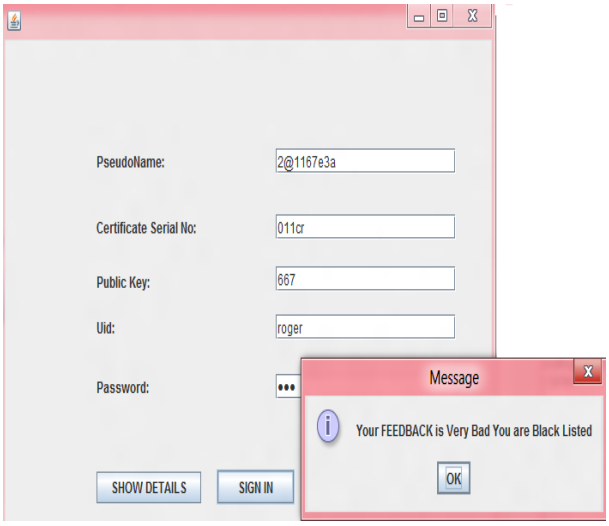

Fig 14: Blackisted user, error message shown when logged in

C. Comparative Analysis

Here, our proposed BLACTR is compared with BLAC and BLACR. For the purpose, 50 users are taken and the total number of edits by these users came about 1000. Each time the user edit is evaluated by the certifying authority and also by other users. Based on the reviews the user is blacklisted or not. In our case, all the edits are recorded and manually evaluated for the purpose of evaluation for our proposed BLACTR. It is found form the manual evaluation that 12 users should be blacklisted based on their edits.

The effectiveness of our proposed BLACTR in comparison to other techniques (BLAC and BLACR) is found out using the parameters deviation and percentage deviation. Better technique will have lower value of parameter and the percentage deviation. Here deviation D is defined as:

$$Deviation$$
$$D = \| B - O \|,$$
$$where\ O\ is\ the\ original\ number\ of\ users\ in\ Blacklist$$
$$B\ is\ the\ number\ of\ users\ Blaclisted\ by\ the\ technique$$
$$Percentage\ Deviation\ P = \frac{D}{O} = \frac{\| B - O \|}{O}$$

T able 1, figure 15 and figure 16 shows the comparative analysis of BLAC, BLACR and proposed BLACTR using deviation and percentage deviation parameters. From the table, it is clear that our proposed BLACTR performs well and has achieved better results by having lower deviation and percentage deviation.

	Number of users Blacklisted(B)	Deviation(D)	Percentage Deviation(P)

BLAC	*19*	*6*	*50*
BLACR	*16*	*4*	*33.3*
BLACTR	*13*	*1*	*8.3*

Table 1

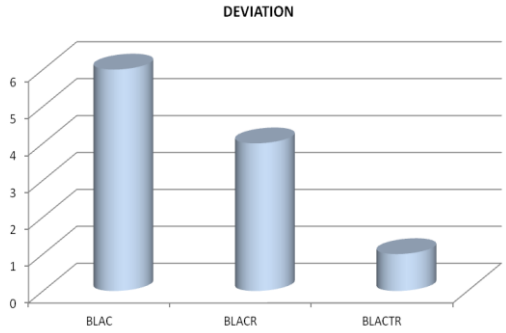

Fig 15: Plot of deviation values

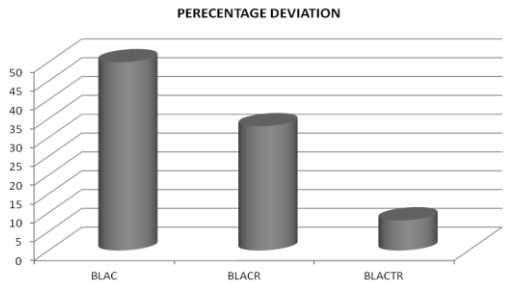

Fig 16: Plot of percentage deviation values

VII. CONCLUSION

In this paper, we propose a technique known as Blacklistable Anonymous Credentials with Trust Reputation (BLACTR) for revoking misbehaving users with Trusted Third Party (TTP). The technique uses both Certifying Authority (CA) review as well as other user reviews in order to blacklist a user making use of the fuzzy in the backend. Initially, the user submits his/her personal details to CA for obtaining either the anonymous or the normal certificate according to the user need. The user is taken to the service provider page where the person will be able to edit the data. The edit can be viewed by the CA and rates the user accordingly. The edit is also rated by other users and then converted to fuzzy and rule matched to check if the person is to be blacklisted or not. The proposed technique performed well when compared to BLAC and BLACR.

REFERENCES:

[1]Jan Camenisch, Anna Lysyanskaya "An Efficient System For Non Transferable Anonymous Credentials with optional Anonymity Revocation",pp 93-118,2001.

[2]Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss,Anna Lysyanskaya,and Hovav Shacham "Randomizable Proofs and delegatable Anonymous Credentials" ,Vol- 5677,pp 108-125,2009.

[3]Dr A. Damodaram,H.Jayasri "Authentication without Identification Using Anonymous Credential System",vol abs/0908.0979,2009

[4]"Digital Credentials" from http://en.wikipedia.org.

[5]JornLapon, MarkulfKohlweiss, Bart De Decker, Vincent Naessens:"Analysis of Revocation Strategies for Anonymous Idemix Credentials," Communications and Multimedia Security, pp. 3-17,2011.

[6] Liu Xin ,XuQiu-liang,"Improved Hidden identity-based signature scheme,"IEEE Conference on Intelligent Computing and Intelligent Systems (ICIS),vol.1,pp.416-478,2010 .

[7]Othman,Hashim,Razmi, Manan," Privacy-Enhanced Trusted Location Based Services (PE-TLBS) framework based on Direct Anonymous Attestation (DAA) protocol,"International Conference onComputer Applications and Industrial Electronics (ICCAIE),pp.297-303,2010 .

[8]Jinyuan Sun ,Chi Zhang, Yanchao Zhang ,Yuguang Fang," An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks,"IEEE Transactions on Parallel and Distributed Systems, vol.21,pp.1227-1239,2010.

[9]Barisch,Garcia, Lischka, Marques, Marx, Matos, Mendez,"Security and privacy enablers for future Identity Management systems"conferrence on Future Network and Mobile Summit,pp.1 - 10,2010.

[10] Coles-Kemp,Kani-Zabihi,"Practice Makes Perfect: Motivating Confident Privacy Protection Practices", ieee third international conference on and 2011 IEEE third international conference on social computing (socialcom),pp. 866- 871 ,2011.

[11]Patrick P. Tsang, Man Ho Au, Apu Kapadia, and Sean W. Smith. "Blacklistable anonymous credentials: blocking misbehaving users without TTPs". In Ning et al. [27], pages 72 { 81.

[12] Man H. Au, Apu Kapadia, Willy Susilo, "BLACR: TTP-Free Blacklistable Anonymous Credentials with Reputation", In Proceedings of the 19th Annual Network & Distributed System Security Symposium, May 2011.

[13] I.Teranishi and K.Sako, " K-times Anonymous Authentication with a Constant Proving Cost",In

Public Key Cryptography, vol 3958 of LNCS pp 525-542,2006.
[14] I.Teranishi, J.Furukawa and K.Sako,"K-times Anonymous Authentication (extended abstract) in ASIACRYPT, vol 3329 of LNCS, pp 308-322 ,2004.

Authors

Dr Avula Damodaram obtained his B.Tech. Degree in CSE in 1989, M.Tech. in CSE in 1995 and Ph.D in Computer Science in 2000 all from JNTUH, Hyderabad. His areas of interest are Computer Networks, Software Engineering, Data Mining and Image Processing. He has successfully guided 6 Ph.D. and 2 MS Scholars apart from myriad M.Tech projects. He is currently guiding 9 scholars for Ph.D and 1 scholar for MS. He is on the editorial board of 2 International Journals and a number of Course materials. He has organized as many as 30 Workshops, Short Term Courses and other Refresher and Orientation programmes. He has published 35 well researched papers in national and International journals. He has also presented 45 papers at different National and International conferences. On the basis of his scholarly achievements and other multifarious services, He was honored with the award of DISTINGUISHED ACADAMICIAN by Pentagram Research Centre, India, in January 2010.

H.Jayasree obtained her B.E. in CSE from Bangalore University and M.Tech. in CSE from JNTUH, Hyderabad in 2001 and 2006 respectively. She is currently a Research Scholar of CSE JNTUH, Hyderabad. She is working as Associate Professor, for Aurora's Technological and Research Institute and has 10yrs of teaching experience in various colleges of Hyderabad and Bangalore. Areas of research interest include Computer Networks and Network Security.

