JES
Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

A SMART HEALTHCARE APPLICATION USING PROTECTING THE PRIVACY OF PATIENTS IN CLOUD

[1]Bader Fatima Naaz, [2]Dr.K.Saravanan
[1]PG Scholar, MTech, Dept of CSE, Shadan Women's College of Engineering and Technology HYD, T.S.
baderfatimanaaz@gmail.com
[2]Professor, Dept of CSE, Shadan Women's College of Engineering and Technology HYD, T.S.

Abstract—Many brilliant healthcare applications are embracing cloud to give administrations to patients. Be that as it may, the delicate information can be uncovered to the authentication server/specialist co-op. In this manner, security and protection are pivotal to its prosperity and organization everywhere scale. Patients would prefer not to uncover their characters to the cloud server. One approach to shield their characters from cloud server is mysterious authentication. The authentication procedure typically includes unveiling clients' private data, for example, username and secret key to the authentication server. In the event that the patient can be connected or followed by the authentication server or pernicious foes by their solicitations, their security can be broken. A large portion of the current security saving health care applications give anonymity from the foes. Nonetheless, not very many of them give anonymity from the authentication server. In this paper, we have proposed a framework which gives total security and anonymity to the clients of health care applications from foes and the authentication server. In our proposed authentication conspire, we have used Identity based Encryption (IBE) to give anonymity to the patients. To include an additional layer of security, we have utilized The Onion Router (TOR) to give protection at the system layer. The presentation of our plan is assessed by hypothetical examination which exhibits that it opposes different assaults and gives a few alluring security highlights.

Index Terms—Anonymous authentication,Identity based Encryption, smart health applications

I. INTRODUCTION

Late advances in biosensors, remote system and inserted frameworks have helped the quick improvement of a wide scope of wearable and implantable sensors in the human body. To gather pivotal health information, for example, circulatory strain level, and pulse, many advanced mobile phone based health applications have been created in the ongoing past. The information from the sensors is sent to the cloud server, where emergency clinics have facilitated their administrations for information handling. The information is examined to improve the dimension of healthcare given to the patients. A case of keen cloud based health applications is appeared in Fig. 1. Preferably, patients need emergency clinics to help them with high effectiveness without uncovering patients' characters. The expanding need for huge calculation and extreme amounts of capacity, is driving the healthcare business to utilize cloud based servers, in light of numerous points of interest they are putting forth, for example, cost sparing and scalability. Notwithstanding, sharing information on un-trusted mists can put patients protection in danger. Distributed computing can likewise result in genuine cloud explicit security issues, for example, losing physical power over your information. Unless we give total security and privacy, patients will dependably dither to exchange their private or delicate information to the cloud. There are a few difficulties which we should defeat for structure a dependable and secure information stockpiling/handling framework for healthcare applications on the cloud. These difficulties are as per the following

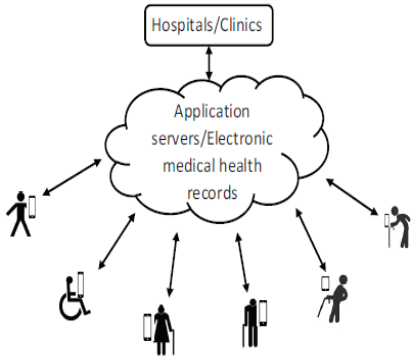

Fig. 1. An example of typical smart healthcare system.

- **Losing physical control:** Outsourcing the information to the mists decreases the capital and operational consumption. Notwithstanding, the dangers related with losing physical command over information must not be disregarded. We have to construct components to secure clients' protection and ensure their classification and uprightness.
- **Multi-tenure:** Due to virtualization, it is presently conceivable that different clients share the equivalent physical capacity, with the assistance of some asset assignment approach. It is generally simple for a malignant client to wrongfully get to information that does not have a place with him in such a domain.

- **Security rupture:** Due to gigantic preparing power, customary systems to ensure a person's protection may not be adequate. For example, our online exercises uncover a great deal about us. Cloud server or any busybody examining our perusing propensities and area impressions can be extremely perilous.

In rundown, because of the exponential utilization of shrewd gadgets a lot of clients' information are created, put away, and prepared on cloud expanding the danger of protection infringement. The keen gadgets and cloud servers not just gather individual data of the clients, for example, a username, secret phrase, and phone numbers however can likewise screen clients' exercises, for example, shopping inclinations and access history. Every one of these dangers related with brilliant cloud based applications have driven analysts to concentrate on applications with solid protection.

A. Motivation

To get to the healthcare administrations online, for example, checking endless maladies (i.e., Cancer, diabetes, asthma, dementia and so on.), a patient must verify himself/herself. The authentication procedure ordinarily includes uncovering the personality of a client, for example, username and secret phrase. In view of the data gave to the cloud server amid the authentication procedure, the patient can be connected or followed utilizing their entrance history or inclinations. As of late, numerous protection safeguarding authentication plans have been proposed . In any case, these plans don't give total anonymity. The point of our exploration is to enable patients to utilize healthcare administrations without uncovering their personalities or being followed by a meddler.

In numerous situations, clients pay the enrollment charge for a specific amount of time to be qualified to utilize the administrations until their participation terminates. For example, an individual from emergency vehicle administration can utilize rescue vehicle administrations at whatever point required all through his/her participation. Following are a few models where the proposed plan can be utilized successfully

- The patients can book a meeting with a healthcare expert or call a rescue vehicle if there should arise an occurrence of crisis utilizing the advanced mobile phone without uncovering their characters.
- In remote health care observing, data of intrigue like circulatory strain level or pulse is accumulated by the sensors joined to the body and transmitted by a controller (cell phones or individual advanced associates) to a server where it is prepared. Consider a case of a patient where an application raises a caution naturally when the readings from the sensors go over the limit. For instance, important specialists (i.e., emergency vehicle administration) can be told when patient's pulse goes over the edge with the endless coronary illness or at whatever point a patient with dementia in helped living offices leaves their characterized boundaries on a given guide.

The character protection of a patient can be ruptured straightforwardly or in a roundabout way. Direct security infringement includes uncovering individual data, for example, username, biometric highlights and so forth., utilized amid the authentication procedure though, circuitous infringement includes removing the data from the shrouded examples, for example, investigating the Internet traffic or patient's inclinations. To safeguard personality security of the patient, numerous extra connections among patient and authentication server should likewise be concealed amid the communication rounds between them. We mean to accomplish the accompanying highlights in our proposed mysterious authentication plot:

- Anonymity: The patient must almost certainly validate namelessly with authentication server without uncovering his own subtleties.
- Unlinkability: The authentication server and listen in per ought not have the option to connect whether at least two authentication demands are originating from a similar patient. in the event that different demands by a similar patient can be connected together by a meddler or authentication server, the patient might be distinguished.
- Traceability: It is imperative to recognize the client sometimes. Giving total anonymity to the patients sounds exceptionally engaging yet in addition has some genuine ramifications. Total anonymity for the framework can be accomplished at the expense of trading off evaluating process which implies reviewing for the framework is absurd. For instance, a malevolent patient can over-burden the framework with phony arrangement appointments or unnecessary emergency vehicle calls and we will have no real way to discover the wellspring of the noxious solicitation. Notwithstanding, for down to earth application situations, this isn't the perfect case. We need a component which gives most extreme anonymity to the patients as long as they don't get out of

hand. In the event that the patient acts up, his character ought to be uncovered and his enrollment could be disavowed if vital.

- ❖ Resistance to attacks: It is significant for a framework to be impervious to every conceivable assault i.e., spying, replay attacks, man in the center assault and so forth.
- ❖ Integrity: The transmitting messages ought to be irrefutable by the accepting party.

The essential objective of this paper is to give character security to keen cloud based healthcare applications by giving mysterious authentication. The proposed plan can be summed up and connected to other cloud based applications. In certain situations, client can conceivably be distinguished by the activities performed on a particular arrangement of information after some time. In this manner, the proposed plan is most reasonable for situations where the particular client can't be recognized by tasks over the information. It is significant that different issues, for example, area security and question protection in savvy health application are similarly significant. Be that as it may, the investigation of those issues is outside the extent of this work.

II. RELATED WORK

The related work on mysterious authentication plans can be extensively characterized into public key cryptosystems (PKC) based plans, personality based cryptosystems plans, nom de plumes plans, consolidated plan utilizing both character based encryption and nom de plumes, application arranged plans. Mysterious authentication plans dependent on PKC in, were infeasible for portable networks in light of the computational assets required by PKC particular exponentiation, which devour a larger number of assets than what a cell phone can offer. To limit the computational necessities, different mysterious authentication plans dependent on Identity based Encryption have been proposed, which have better execution on account utilized in IBE.

Mysterious authentication plans are also developing through the use of nom de plumes different systems to ensure protection. Sun et al. offered answers for protection and crisis reaction dependent on the mysterious credential, pseudo-irregular number generator, and the information of confirmation for distributed frameworks. Notwithstanding, when straightforwardly connected to the circulated healthcare framework, these plans are impractical because of overwhelming computational overhead. In, Lin et al. proposed a solid protection safeguarding plan against global spying (SAGE), using nom de plumes personality-based encryption to build the dimension of security. This plan gives both substance and setting focused protection opposing solid global foe.

As of late, two factor (secret key and smartcard) authentication plans have been proposed. Notwithstanding, these plans have confinements as the smartcard and secret key both can be lost, stolen or copied. Also, a portion of these plans require the server to keep up a secret key table for check purposes, making them experiences some potential attacks such secret key divulgence attacks and server parodying attacks. To handle the issues in two factor based authentication plans, three factor (biometric, secret word and keen card), authentication plans have been proposed. To upgrade the security, biometric qualities are utilized as a third factor to plan a solid authentication plot. These plans are intended for savvy cards. Be that as it may, brilliant cards can't perform progressively modern undertakings like interfacing with the server or communication with the server in this manner, these plans are not appropriate for authentication utilizing advanced mobile phones.

In, a mysterious authentication plot in the cloud condition for e-health has been proposed. The plan in depends on blind marks which allow clients to devour cloud benefits secretly. The plan does not give any details about client enlistment and revocation. The security analysis of the plan isn't talked about in detail.

In, mysterious authentication plans for wireless body area networks (WBANs) were proposed. The plan in depends on bilinear pairings and it proposed a proficient unknown verified key understanding plan for WBANs. The plan in depends on declaration less encryption, which was intended to dispose of the disadvantages of the PKI based plans. It doesn't require digital testament and character based encryption, i.e., no key escrow issue. The plans in were both effective, in any case, revocation was not unmistakably characterized.

In, a mysterious authentication conspire was proposed for wireless networks utilizing Verifier-Local revocation (VLR) bunch signature plot. Be that as it may, the plan in is helpless against replay attacks and a malicious Group Manager can imitate a client.

Also, the unknown authentication plans dependent on gathering marks have been proposed in numerous areas. The gathering mark plans have been generally utilized in vehicular specially appointed networks (VANETs) to realize unknown authentication. To improve the contextual mindfulness, the vehicles communicate with one another by communicating safety messages with position reference points. What's more, the gathering marks are utilized to ensure the personality of the clients sending safety messages to secure the area and

character protection. In, the gathering marks are utilized to protect security in pervasive social networking (PSN), where PSN underpins moment social exercises at whenever and anyplace. The mysterious authentication is accomplished by confirming the trust levels as opposed to the characters of hubs. The plan accomplishes anonymity and conditional traceability by using bunch marks and with the help of Trusted Authority (TA). Be that as it may, the mysterious authentication plots in are altogether different in setting to our proposed plan.

The vast majority of these previously mentioned plans give anonymity from the spy. In any case, the specialist organization is as yet ready to extricate the real character of the client to give him access to the administrations and can link different messages originating from a similar client.

III. OUR CONTRIBUTION

To provide the services to the patients while maintaining privacy, we propose an anonymous authentication scheme utilizing based on IBE, which is both secure and efficient. Our contributions can be summarized as the following modules:

- User Interface
- Group Manager
- User
- Cloud Service Provider
- Services

DESCRIPTION:

- **User Interface**

This is the first module of our project. The important role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

- **Group Manager**

Group Manager is a first module of this project. This GM is the owner of the hospital. In this module GM login, and then view the all users request and accept the users and generate ID to that users. GM sends accepted user's details to cloud service provider to provide the hospital services to the users. And GM also add the doctors based on the diseases. He can view the total doctors details.

- **User**

User is the second module of this project. In this module user can register with Group Manager. Send request to get the ID after getting ID user can login to the site, send request to the Cloud Service Provider to access the hospital services. After receiving the key from CSP, user can use the services. If the user is authenticated then only he can use the services otherwise that user is deleted/removed by the CSP.

- **Cloud Service Provider**

Cloud Service Provider is the third module of the project. CSP login and he can view the patient request , if the patient is authorized then only key will generated to the patient otherwise he can removed without using the services.

- **Services**

Services are the fourth module of the project. In this module patient can login into the services page and he can view the services provided by the GM/Hospital based on his requirement he can send request to the particular service to access.

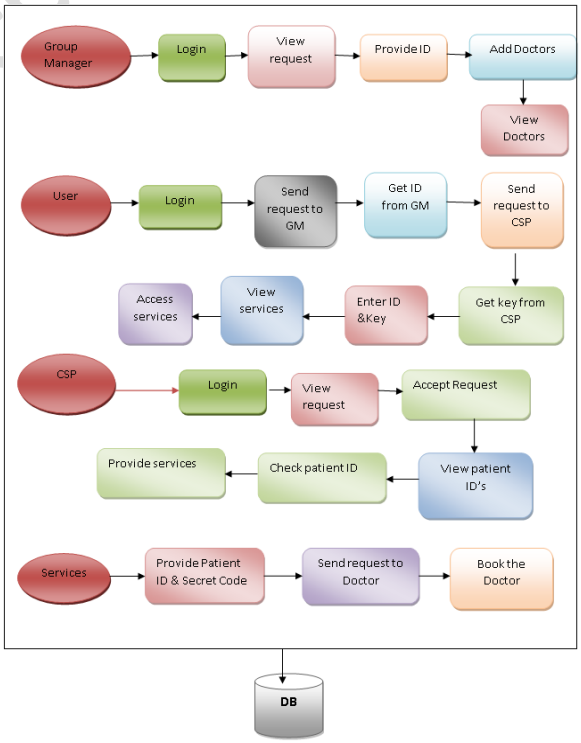

Fig. 3: System Architecture

Journal of Engineering Sciences
Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

ALGORITHM:

STEP 1: Initially algorithm IBE run by key authority means Group Manager. Takes input security parameters. Output parameters like private key. And store details in revocation list.

Input: register with unique id with email

Output: Group Manager maintains revocation list.

STEP 2: private key generation algorithm run by Group Manager and takes input public parameters of users like email, mobile number etc..

Input: login with email id and password are public parameters

Output: Group Manager authenticate user and generates ID.

STEP 3: The key generation is done by Cloud Provider takes input parameters as ID and check

The user authentication with Group Manager and generate the private key to user.

Input: user send request to Cloud provider with Group Manager generated ID

Output: Cloud Provider checks user authenticity and generate private key.

STEP 4: The revocation algorithm run by Group Manager takes input identity to be revoked.

Check in revocation list and delete the user if the user misbehaves with the network.

Input: Group manager login and view list of users

Output: Revoke any user if they misbehave.

IV. RESULTS

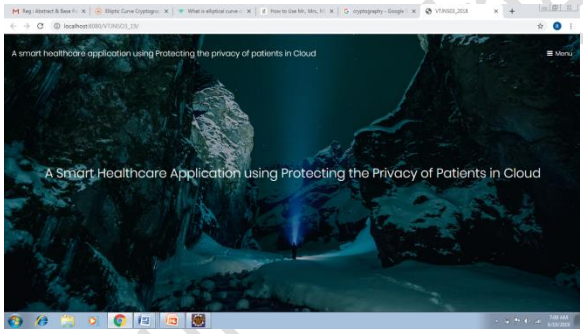

Fig. 4: Application Home Page

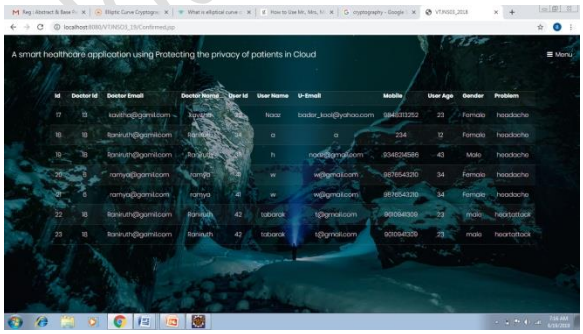

Fig. 5: All Data Page

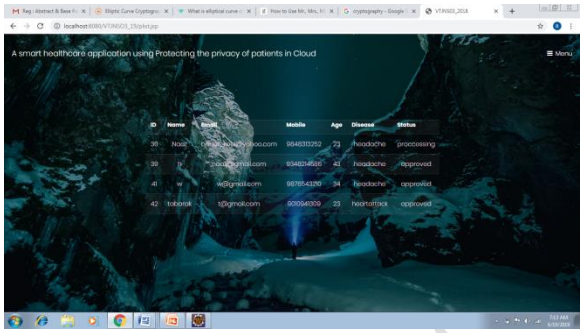

Fig. 6: All Patent Records

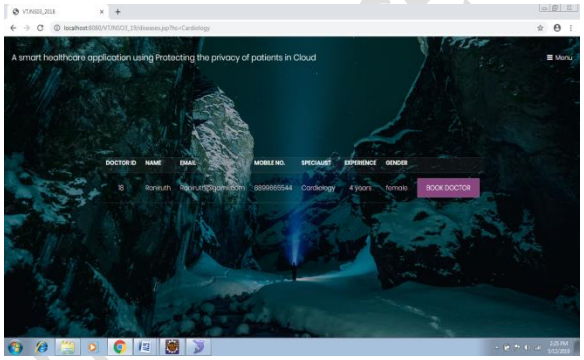

Fig. 7: Request Details

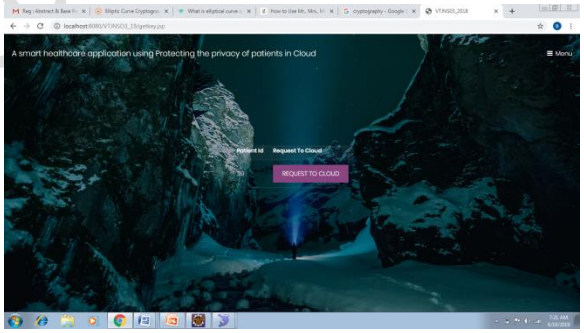

Fig. 8: Request to Cloud Page

V. CONCLUSION

Ensuring the security of patients is crucial to the accomplishment of brilliant cloud based healthcare applications. In this paper, we have introduced the mysterious authentication conspire for keen cloud based healthcare applications. The proposed plan safeguards the security of patients when they get to the administrations facilitated on the cloud. The plan uses IBE the security of the framework can be effectively scaled up by without influencing the computational unpredictability. The plan includes an additional layer of security against traffic analysis attacks by a spy by giving anonymity at the network layer by utilizing TOR. The plan shields patients' touchy information from a meddler and untrusted cloud servers. One salient component of our plan is that the medical application or specialist co-ops can't

reveal the personality of the patient consequently securing the protection. In this paper, we have structured a practical framework which is secure and productive. The proposed authentication conspire guarantees that the patients can devour administrations without revealing their personality at the season of utilization or retrospectively.

REFERENCES

[1]A. Martinez-Balleste, P. A. Perez-Martinez, and A. Solanas, "The pursuit of citizens' privacy: a privacy aware smart city is possible," IEEE Commun. Magazine, vol. 51, no. 6, pp. 136–141, Jun. 2013.

[2]D.Aranki, G. Kurillo, P. Yan, D. M. Liebovitz, and R. Bajcsy, "Real-time tele-monitoring of patients with chronic heart-failure using a smartphone: lessons learned," IEEE Trans. on Affective Computing, vol. 7, no. 3, pp. 206–219, Apr. 2016.

[3]Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Commun. Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, May 2013.

[4]D. Ding, M. Conti, and A. Solanas, "A smart health application and its related privacy issues," in Proc. Smart City Security and Privacy Workshop (SCSP-W), Apr. 2016, pp. 1–5.

[5]P.Gope and T. Hwang, "Untraceable sensor movement in distributed iot infrastructure," IEEE Sensors J., vol. 15, no. 9, pp. 5340–5348, Jun. 2015.

[6]X.Su, J. Hyysalo, M. Rautiainen, J. Riekki, J. Sauvola, A. I. Maarala,

H. Hirvonsalo, P. Li, and H. Honko, "Privacy as a service: Protecting the individual in healthcare data processing," Comput., vol. 49, no. 11, pp. 49–59, Nov. 2016.

[7]W. Lei, Y. Li, Y. Sang, and H. Shen, "A secure anonymous authentication scheme for electronic medical records system," in Proc. 13th Int. Conf. on e-Business Engineering, Nov. 2016, pp. 48–55.

[8]V.Sucasas, G. Mantas, A. Radwan, and J. Rodriguez, "An oauth2-based protocol with strong user privacy preservation for smart city mobile e-health apps," in Proc. IEEE Int. Conf. on Commun., May 2016, pp. 1–6.

[9]R. Fernando, R. Ranchal, B. An, L. B. Othman, and B. Bhargava, "Consumer oriented privacy preserving access control for electronic health records in the cloud," in Proc. IEEE 9th Int. Conf. on Cloud Computing, Jun. 2016, pp. 608–615.

[10]A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, "Protection of big data privacy," IEEE Access, vol. 4, pp. 1821–1834, Apr. 2016.

[11]H.Xiong, J. Tao, and C. Yuan, "Enabling telecare medical information systems with strong authentication and anonymity," IEEE Access, vol. 5, pp. 5648–5661, 2017.

[12]X. Li, S. Tang, L. Xu, H. Wang, and J. Chen, "Two-factor data access control with efficient revocation for multi-authority cloud storage system," IEEE Access, vol. 5, pp. 393–405, 2017.

[13]J. Zhu and J. Ma, "A new authentication scheme with anonymity for wireless environments," IEEE Trans. on Consumer Electron., vol. 50, no. 1, pp. 231–235, Feb. 2004.

[14]G. Horn and B. Preneel, "Authentication and payment in future mobile systems," Comput. Security – ESORICS 98, pp. 277–293, 1998.

[15]C. Yang, W. Ma, and X. Wang, "Novel remote user authentication scheme using bilinear pairings," Lecture Notes in Comput. Science, vol. 4610, p. 306, 2007.

[16]P. E. Abi-Char, A. Mhamed, and E.-H. Bachar, "A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications," in Proc. Int. Conf. on Next Generation Mobile Applications, Services and Technologies, 2007, pp. 235–240.

[17]L. Zhang, S. Tang, and H. Luo, "Elliptic curve cryptography-based authentication with identity protection for smart grids," PloS one, vol. 11, no. 3, pp. 1–15, 2016.

[18]Y.-M. Tseng, T.-Y. Wu, and J.-D. Wu, "A mutual authentication and key exchange scheme from bilinear pairings for low power computing devices," in Proc. 31st Annu. Int. Conf. on Comput. Software and Applications, vol. 2, Jul. 2007, pp. 700–710.

[19]J.-H. Yang and C.-C. Chang, "An id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," Comput. and Security, vol. 28, no. 3, pp. 138–143, Jun. 2009.

[20]X. Cao, X. Zeng, W. Kou, and L. Hu, "Identity-based anonymous remote authentication for value-added services in mobile networks," IEEE Trans. on Vehicular Technology, vol. 58, no. 7, pp. 3508–3517, Sep. 2009.

[21]R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "A novel anonymous mutual authentication protocol with provable link-layer location privacy," IEEE

Trans. on Vehicular Technology, vol. 58, no. 3, pp. 1454–1466, Mar. 2009.

[22]I.Teranishi, J. Furukawa, and K. Sako, "K-times anonymous authentication," IEICE Trans. on fundamentals of Electron., Commun. and Comput. Sciences, vol. 92, no. 1, pp. 147–165, Jan. 2009

AUTHOR'S PROFILE

BADER FATIMA NAAZ has completed her engineering (B.E (IT)) from Muffakham Jah college o fengineering and technology, Banjara hills Hyderabad. OU University Hyderabad. Presently, she is pursuing her Masters , Dept of CSE from Shadan womens college of Engineering and technology, Hyderabad, TS. India.

Mr.DR. K. SARAVANAN received the Ph.D degree in Information and CommunicationEngineering from Anna University, Chennai. He has 12 years of teaching experience. His areas of interest include information security, Adhoc Networks and Network Security. At present he is working as a professor in Departmentof Computer Science and Engineering at Shadan Women's College of Engineering and Technology, Hyderabad. Hehas published 28 papers in International Journal, 30 papers in National and International Conferences. He is anactive reviewer in Elsevier, Springer, Inderscience and many other journals.