International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-5, January 2020

A Prototype Model of Virtual Authenticated Key Exchange Mechanism over Secured Channel in Ad-Hoc Environment

S. Malathi, C. Mohan, M. Arun, R. Kalpana, M. Athigopal

Abstract: ***Key exchange protocols play a vital role in symmetric key cryptography. The transfer of private key through the secured medium is a challenging task because every day the intruders are evolved and the attacks are increasing constantly. The existing key exchange protocols such as Diffie-Hellman, Elgamal, and MQV, etc. are the old methods and many attacks happened on those protocols. That challenges demanding new protocol or methodology of transferring secret key between the parties. The paper proposes a new, secured, less computational overhead key exchange mechanism using short message service available in the cellular networks. GSM-SMS is a highly established secured channel and the research uses this facility to transfer the key between senders to a receiver of the symmetric key cryptosystem. The private key no need to reveal to third parties or even the receiver because the sender can directly communicate to the decryption system through the mobile SMS. After the decryption process, the secret key will be destroyed immediately. There is no possible attack during the key transfer and loss and error of the communication are very less.***

Keywords: ***Cryptography, Key exchange protocol, Mobile Environment, SMS.***

I. INTRODUCTION

In general, cryptography is the traditional way of protecting information and it has been a crucial mechanism from the ancient period [1]. The cryptography has been civilized by various great mathematicians and scientists from various periods [2]. After the revolution of the computer era, it has been computerized and equipped with various algorithms continuously. Computer security is a vast area and it plays a significant role in data transfer and storing information. Hereafter this text means only computer cryptography.

Manuscript published on January 30, 2020.
* Correspondence Author
S. Malathi*., Assistant Professor, Sri Krishna Adithya College of Arts and Science, Coimbatore, India.
Dr. C. Mohan., Assistant Professor in Department of Computer Science, The American College, Madurai, India.
M. Arun., Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India
R. Kalpana., Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India
M. Athigopal, Assistant Professor in Subbalakshmi Lakshmipathy College of Science, Madurai, India.

Widely, the cryptography divided into two main categories that are symmetric key encryption and asymmetric key encryption that can be called private key public key cryptography respectively. The symmetric key algorithms use a single key for both encryption and decryption; it is called a private key. Instead, an asymmetric algorithm uses two separate keys for encryption and decryption, called the public key.

The symmetric algorithm needs to transfer key to the receiver and it required a secured medium and secured mechanism called key exchange protocol [3]. Widely used symmetric key algorithms are Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Kuznyechik, RC4, DES, 3DES.

Diffie-Hellman is the pioneer of a key exchange protocol [4]. It uses an algorithm to secure the key and now it becomes vulnerable. There are several types of research that are proposed to overcome the existing problems and they all have different uniqueness. This paper proposes a novel mechanism for exchanging the private key through mobile SMS. The authenticated person can be decrypting the ciphertext from a remote place without revealing the key to anyone. The key will transfer through a defined GSM SMS secured channel. Established security is used to transfer the key.

The paper further organized into 8 chapters and the first two chapters are introduction and literature review. The review focuses only on password, session and certificate-based results. Chapter 3 introduced the proposed architecture and its modules. Chapter 4, 5 explained the working procedure of the proposed mechanism. The result and performances are discussed in chapters 6 and 7. The conclusion will be given in the last chapter.

II. LITERATURE REVIEW

The review try to explore some of the identical researches which is related to key exchange protocols and it limit the coverage based on identity-based, password-based, session-based and certificate-based. These researches are contributed significantly towards the efficient and high secured key exchange mechanism (fig 1).

Fig 1 Overview of Literature review

Kisung park et al [5] proposed a new secure and efficient scheme 2PAKEP that is a two-party authentication key exchange protocol and it overcomes the security weaknesses of Qi and Chen's scheme [6].

The proposed scheme overcomes the existing key exchange vulnerabilities that are the prevention of impersonation, password change, privileged insider, offline password guessing attacks. Even the existing proposal does not support the anonymity, secure mutual authentication, secure key agreement, and efficient password change mechanism. Subsequently, the proposed model overcomes the above limitations and vulnerabilities. In 2PAKEP, the overall process is logically divided into 3 phases that are

User registration – all the mobile network users should register on the server.

Exchange of key and mutual authentication– the registered users sends a request to the server to exchange the key.

Change of password activity – the mobile user can be changing their password through the requisition to the server.

The paper compares security, computational overhead, and communication overhead against the several existing methods; all the result provides better results than others.

Liu Xiumei et al [7] introduced a new password-based authenticated protocol called verifier based n-party password-authenticated key exchange (VB-nPAKE). Its support N client and each client generate a pair of keys and it will decrypt by their password. The verifier will share with both parties and it will seem to be a public key. The author proves that this protocol overcomes various conventional attacks through security analysis.

A. Abusukhon et al [8] proposed an enhanced multi session-based authenticated key agreement protocol which is resolving the limitation of the existing protocol like HMQV and YAK. The proposed protocol works based on the protocols of Menezes-Qu–Vanstone (MQV) family and Elliptic Curve-Diffie Hellman (ECDH) [9].

J. Wu et al [10] suggest a new session-based protocol named ID-CL-eCK that is an identity-based authenticated key exchange and this is the advancement of LR-ID-AKE. The leakage resilient based researches are carried out by [11 –14] and the proposed protocol is the advancement of that research. The public key generator (PKG) generates two different keys for sessions and it will exchange to the users.

That key generations happen in the setup phase and extract phase used to identify the key and user and session phase establish the connection between the user (fig 2).

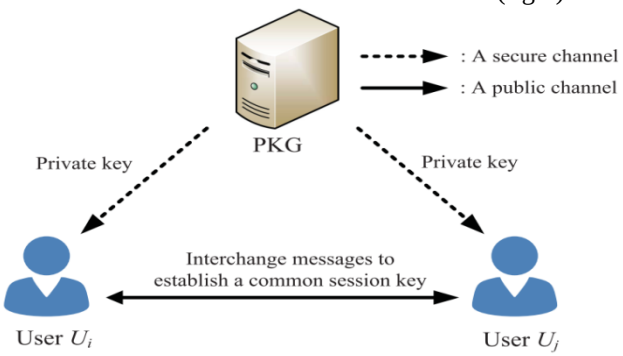


Fig 2. Framework of the LR-ID-AKE protocol [x6]

The author [15] proposed a certificateless non-interactive key exchange protocol to improve the efficiency of interactive key exchange. It proves its efficiency during the testing on the random oracle model and reduces the gap of Diffie-Hellman (GDH) and computational Diffie-Hellman (CDH) problem.

Swapnil paliwal [16] introduced a hash value based key exchange protocol in industrial IoT. Data transfer in IoT is the most vulnerable and it could be overcome by authenticated key exchange. This architecture reduces computational overhead and complexity.

X. Yi et al [17] suggest identity-based signature authentication and key exchange protocol between the compilers. The research is the precedence of Paterson et al [18] research and it uses two different private key and can be exchanged between the compilers and authenticate.

III. MUTUAL KEY EXCHANGE SCHEME

In symmetric cryptography, the private key needs to be transferred to decrypt the cipher text. The method of exchanging key is most challenging and needs to be transferred with a secured channel. The channel can be any medium (wireless or wired) or person. The proposed scheme uses short message services to exchange the private key to the destination party (fig 3). The working principles of the proposed system can be classified into

- Encryption,
- Decryption
- Mobile interface.

The whole encryption and decryption processes are executed in encryption and decryption part. Mobile interface is the core part of this architecture because it manages all the activities of decryption and key exchange mechanism automatically.

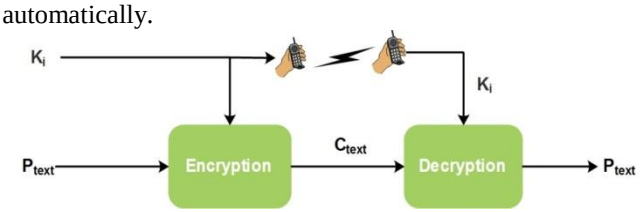


Fig 3. Overview of PK-KEP

The SMS based key exchange mechanism is the most secure and less vulnerable. The user can encrypt the plain text (P_{text}) using any of symmetric algorithms like DES, triple DES, etc. once the plain text is encrypted using a private key (K_i) and ciphertext C_{text} can be transferred to destination with normal procedure, but the exchange of key between the parties is different. The key should not transfer physically in this scheme instead that can be transferred through mobile SMS from the authorized mobile phone. The sender does not show or reveal the key to anyone, the sender itself decrypt thorough this scheme.

The key exchange medium is GSM SMS and the mobile interface will take care of all activities like listening to the incoming message from the particular phone, decoding the key from the SMS, decrypting ciphertext, deleting the key and so on.

The (K_i) will immediately delete from the phone memory and inbox after decryption is done. Both the encryption and decryption are done by using the mobile interface (fig 4).

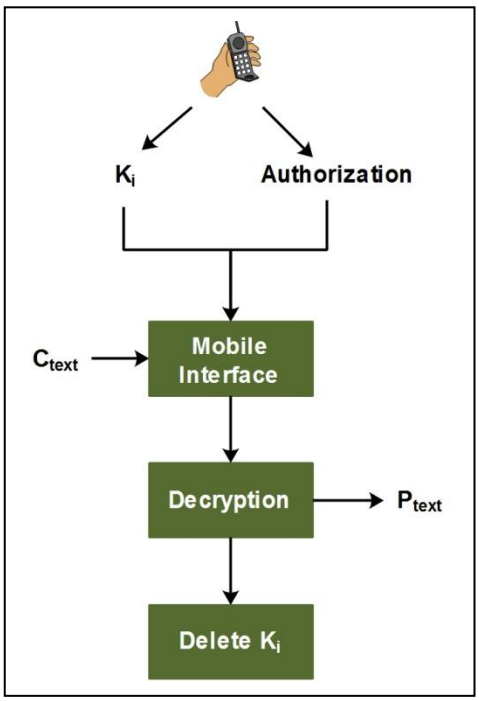


Fig 4 Working principle of mobile interface

IV. ENCRYPTION AND DECRYPTION

The encryption can be done through the PK-KEP model because the model allows the user to choose any one of the symmetric key algorithm to encrypt and decrypt. The sender can encrypt the plain text (P_{text}) and the P_{text} can be in any text file or can enter directly through the interface. The model provides an advanced and compact software interface to do all the cryptography activities. The software interface provides the facilities to choose the external text file or can give input directly. Usually, the K_i is set by the sender and it can be 32-bit, 64-bit or 128-bit, etc. the secret key is defined in the medium of a text file which is hidden by the software interface. Usually, the software interface keeps K_i at the source directory. The C_{text} will be stored in a separate file named encrypt. This file is automatically generated by the software interface and stored in the source directory. Once the encrypted file is generated, the file can be transferable to anywhere and it will be decrypted only through the PK-KEP software interface because the input K_i is further modified by adding the authorized 10 digits mobile phone number. The system is designed to check the mobile number then employ K_i, so it acts as two-level security. Here C'_{text} represents the ciphertext before the mobile number going to add. M_i represents any 10 digits authorized mobile number.

$$P_{text} + K_i \rightarrow C'_{text} \quad \text{Equation (1)}$$

$$C'_{text} + M_i \rightarrow C_{text} \quad \text{Equation (2)}$$

During the decryption, the mobile interface reads the incoming message from the authorized mobile phone with the key. The SMS has to be a particular format and then it will be processed by the interface. The cipher text can be found in the source directory and apply the decryption algorithm which already been used for encryption. If the incoming SMS is from the authorized phone then only it checks the key, if the key is wrong then it does not do anything on the cipher text else do the procedure.

V. MOBILE INTERFACE

This is the core part of the model. This interface creates a connection between the GSM modem and the software module. The GSM modem is responsible for send and receives the SMS through AT commands. The mobile interface creates a connection through cable or wireless connection. If the user connects the mobile phone to the system, then it needs connection by cable or any wireless connection. If the user connects the GSM module then it will connect through cable only. Once the connection will establish through the COM port then the software module start monitors the modem activities by AT commands (will be discussed in the upcoming section). The interface sends and receives data through these COM ports only. Phone specific commands are given as input to the phone interpreter which will process in the phone and will return data on the same port. The active COM port number is generates dynamically by the operating system, this number varies from computer to computer (Fig 5).

When the sender sends the key through authorized mobile with a valid syntax then the SMS will be parsed. The syntax of the incoming SMS should be <# keys> for example '# abcdef123'. This syntax classifies the normal message or special message. If the incoming SMS is a command SMS then it will check the key and if the key is wrong it will do nothing. If the key is correct then the software module calls the decryption algorithm then deletes the special SMS from the phone inbox or memory because nobody can see the key. The software module takes care of phone connection, authorization, validation of incoming SMS, decryption. It will omit the SMS when the wrong key transferred from the authorized mobile and it will not show any key to the outside world when the decryption process is started then the special SMS will erase for security reasons. This method will not show the secret key anywhere or to anyone (Algorithm 1).

Algorithm 1: PK_KEP

Function Encrypt ()

Input: P_{text}, K_i, C_{text}, M_i

Initialize: P_{text} ← input_text; K_i ← private_key;

M_i ←10 digit number; C_{text} ← null

C_{text} ← P_{text} + K_i + M_i

Save C_{text} to local directory

End function

Function decrypt ()

Input: In_SMS, M_i, K_i, C_{text}

If New In_SMS ***then***

If M_i = = authorized ***then***

If In_SMS is Special SMS ***then***

Read K_i

P_{text} ← C_{text} + K_i

Delete K_i and In_SMS

End if

End if

End if

5.1 AT commands

AT commands are instructions used to control a modem. AT is the abbreviation of ATtention. Every command line starts with "AT" or "at". That's why modem commands are called AT commands. These commands were derived from Hayes commands which were used by the Hayes smart modems [19]. Every wireless, as well as the dial-up modems, requires an AT command to interact with a computer machine. AT commands are classified into 4 categories that are Test, Read, Set, and Execution. Among these, this model use only Read and Execute commands because SMS will read and send an acknowledgement to the sender. All command lines must start with "AT" and end with a carriage return character. The frequently used commands are shown in table 1.

Table 1 AT commands

AT Commands	Description
AT+CMGL	List messages
AT+CMGR	Read message
AT+CMGS	Send message
AT+CMGD	Delete message

VI. RESULT ANALYSIS

PK-KEP model is implemented in .net framework 2018 with windows 7. The software interface is designed by advanced designing logic and the mobile interface uses operating system COM port. The software module tested through Redmi 3s. The module having two options that are offline or SMS based control. If the user wants to check the software module then they use offline mode when the testing is successful they can use SMS mode. Both modes are active no need to enable or disable. Figure 5, 6 is the output of the interface.

The user can select the available port list from the ports combo box and then click the connect button. If the port and other properties are correct then the modem is connected to the software interface through wired or wireless connection and it will control by the software module. When the decryption is over the mobile can be disconnected from the software module by clicking the disconnect button. Encrypt and decrypt Button is used to offline tests. The sender sends the decrypted file and the software module to the receiver and when the software is ready on the remote place then the sender can send the key SMS through authenticated mobile number. The authenticated mobile number can be editable by the admin only.

6.1 Measurement of SMS Arrival Rate

In Global System for Mobile Communication (GSM) architecture all the communications are made by set of logical channels. These channels are bot uplink and downlink. The SMS messages are carried on either SD-CCH or SACCH [20] depending on the use of the traffic channel. Traffic Channel (TCH) is responsible for carry the voice and data and the SMS is carried on the SDCCH (stand-alone dedicated control channel).

In this architecture, the GSM module does not commit TCH but it's dedicate to Sending SMS only so it's always use SDCCH to send SMS. The throughput of the SMS is depends on the network traffic and location [20, 21]. So that the delivery of user request and responses is entirely depends on the above parameters.

Let λsms, λι and λv be the arrival rates for received SMS, updation of the location and voice call setup respectively. The arrival rate of this aggregate traffic that uses SDCCH channels is given by

$$\lambda c = \lambda sms + \lambda \iota + \lambda v.$$

Let the mean service time (i.e. channel holding time) of a single SMS message like μ_{sms}^{-1}, and that updation of the location and voice call setup message be μ_l^{-1} and μ_v^{-1} for respectively. The unconditional expected service time of an arriving message is then given by

$$\mu_c^{-1} = \frac{\lambda_{sms}}{\lambda_c} \times \mu^{-1} + \frac{\lambda_l}{\lambda_c} \times \mu_l^{-1} + \frac{\lambda_v}{\lambda_c} \times \mu_v^{-1}$$

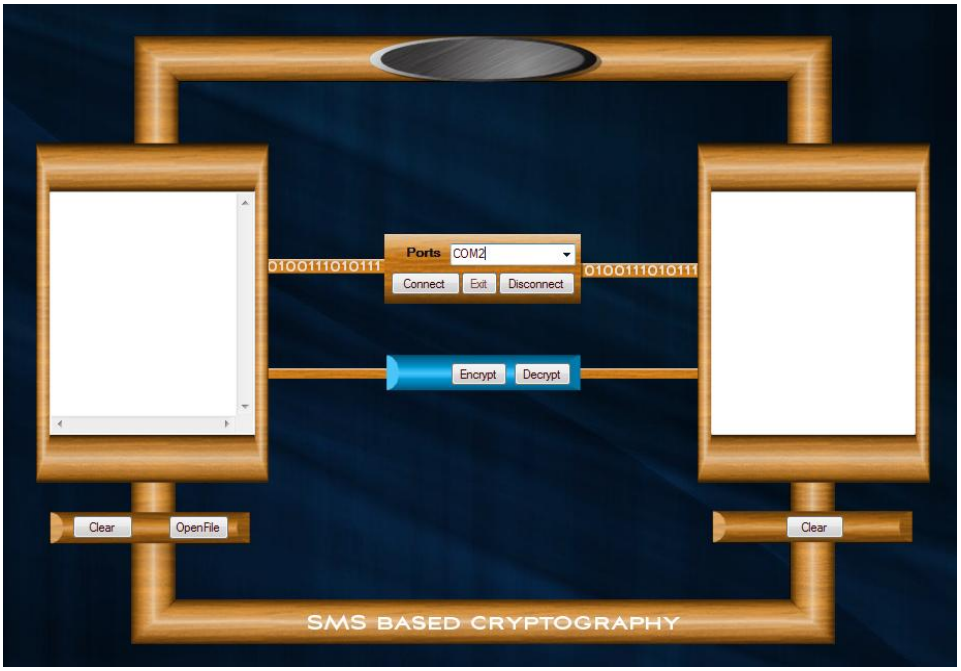


Fig 5. Design of Software Interface

Fig 6. Working state Software Interface

Table 2 (a) SMS delivery time

8.00	8.30	9.00	9.30	10.00	10.30	11.00	11.30	12.00	12.30	13.00	13.30	14.00	14.30
0.03	0.04	0.05	0.05	0.04	0.05	0.04	0.03	0.03	0.04	0.04	0.04	0.03	0.01

Table 2 (b) SMS delivery time

15.00	15.30	16.00	16.30	17.00	17.30	18.00	18.30	19.00	19.30	20.00	20.30	21.00	21.30	22.00
0.02	0.03	0.03	0.02	0.02	0.03	0.03	0.02	0.05	0.06	0.06	0.05	0.05	0.04	0.04

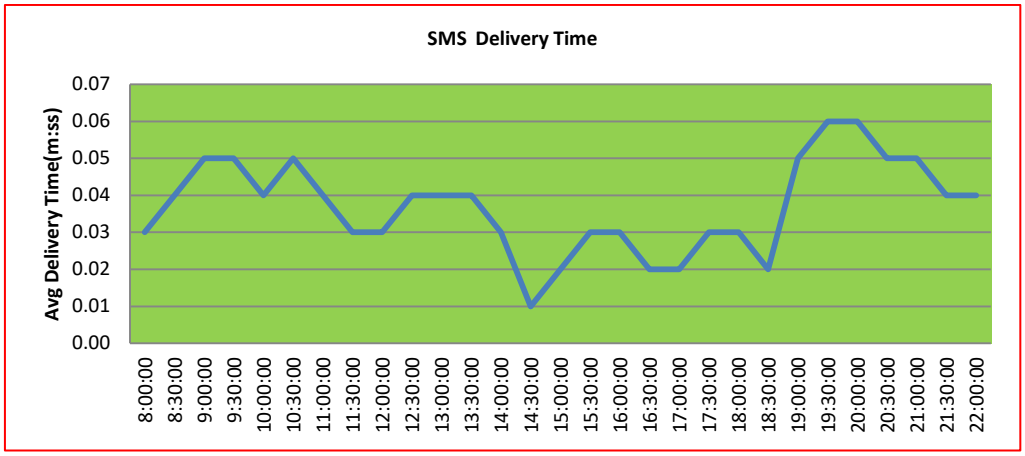


Fig: 7. SMS Delivery Delay Time

Fig. 7 displays the differences of SMS delivery time between 8AM to 10PM. Here the lowest delivery time of special SMS is 1 sec at 2:10PM and the maximum delivery time is 6 sec at 7:50PM. The average delivery time of this architecture is 3.5 seconds and zero data lose.

VII. CONCLUSION

A key exchange mechanism is very important in symmetric key cryptography. Diffie-Hellman, Elgamal, and MQV are the pioneers of key exchange schemes. This paper proposes a new, less computation algorithm to exchange the secret key by using mobile SMS. The security of the exchange medium is already established and tested by 3GPP. The sender does not need to reveal the key instead the one sends the key through SMS by their own mobile phone. Unique software module was developed and tested in the various computing environment. The efficiency of SMS delivery is tested and 3.5 ms is the average delivery time of typical SMS.

REFERENCE

1. Mohd Zaid et al, Evolution of Cryptography, International journal of Evolution of Cryptography, 17 Jan 2007.
2. Takagi, T et al, Mathematical Modelling for Next-Generation Cryptography, Book, 2018.
3. F. Piper, "Basic principles of cryptography," IEE Colloquium on Public Uses of Cryptography, London, UK, 1996, pp. 2/1-2/3.
4. Nan Li, "Research on Diffie-Hellman key exchange protocol," 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, 2010, pp. V4-634-V4-637.
5. K. Park, Y. Park, Y. Park and A. K. Das, "2PAKEP: Provably Secure and Efficient Two-Party Authenticated Key Exchange Protocol for Mobile Environment," in IEEE Access, vol. 6, pp. 30225-30241, 2018.
6. M. Qi and J. Chen, "An efficient two-party authentication key exchange protocol for mobile environment," International Journal of Communication Systems, vol. 30, no. 16, pp. 1–8, 2017.
7. L. Xiumei, G. Kening, Z. Fucai and C. Guiran, "A N-party Diffie-Hellman Key Exchange Protocol Based on Verifier," 2010 International Conference on Communications and Mobile Computing, Shenzhen, 2010, pp. 208-212.
8. A. Abusukhon, Z. Mohammad and A. Al-Thaher, "Efficient and Secure Key Exchange Protocol Based on Elliptic Curve and Security Models," 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2019, pp. 73-78.
9. Brown, D.R. (2014). Some Theoretical Conditions for Menezes-Qu-Vanstone Key Agreement to Provide Implicit Key Authentication. IACR Cryptology ePrint Archive, 2014, 50.
10. J. Wu, Y. Tseng and S. Huang, "An Identity-Based Authenticated Key Exchange Protocol Resilient to Continuous Key Leakage," in IEEE Systems Journal, vol. 13, no. 4, pp. 3968-3979, Dec. 2019.
11. J. Alwen, Y. Dodis, and D. Wichs, "Leakage-resilient public-key cryptography in the bounded-retrieval model," in Proc. Annu. Int. Cryptol. Conf.,2009, pp. 36–54.
12. Y. Dodis, K. Haralambiev, A. Lopez-Alt, and D. Wichs, "Efficient publickey cryptography in the presence of key leakage," in Proc. Int. Conf.Theory Appl. Cryptol. Inf. Secur., 2010, pp. 613–631.
13. G. Yang, Y. Mu, W. Susilo, and D.-S. Wong, "Leakage resilient authenticated key exchange secure in the auxiliary input model," in Proc. Inf.Conf. Secur. Pract. Experience, 2013, pp. 204–217.
14. J. Katz and V. Vaikuntanathan, "Signature schemes with bounded leakage resilience," in Proc. ASIACRYPT, Adv. Cryptol., 2009, pp. 703–720.
15. Y. Wei, F. Wei and C. Ma, "Certificateless non-interactive key exchange protocol without pairings," 2014 11th International Conference on Security and Cryptography (SECRYPT), Vienna, 2014, pp. 1-12.
16. S. Paliwal, "Hash-Based Conditional Privacy Preserving Authentication and Key Exchange Protocol Suitable for Industrial Internet of Things," in IEEE Access, vol. 7, pp. 136073-136093, 2019.
17. X. Yi et al., "ID2S Password-Authenticated Key Exchange Protocols," in IEEE Transactions on Computers, vol. 65, no. 12, pp. 3687-3701, 1 Dec. 2016.
18. K. G. Paterson and J. C.N. Schuldt. Efficient identity-based signatures secure in the standard model. In ACISP'06, pages 207-222, 2006.
19. AT Commands Reference Guide, Telit Wireless Solution, 2006.
20. Pandikumar et al, Secured Policy-based Resource Access and User Authentication in Ubiquitous Computing Environment, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume- 9, Issue-1, July 2019
21. Fabian van den Broek, "Catching and UnderstandingGSM-Signals". Master thesis, Radboud University Nijmegen, March 22, 2010.

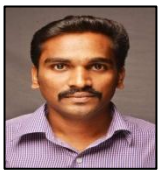
AUTHORS PROFILE

S. Malathi., is working as an Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India. Her area of interest includes Data Structures and Data Mining. She has attended many National Conferences, Workshops and Seminars. She has presented 10 Research Papers in National Conferences and published 7 Research Papers in International Journals.

Dr.C.Mohan., MCA.,Ph.D. is working as an Assistant Professor in Department of Computer Science, The American College, Madurai, India. He has 10 years of teaching experience. He published 10 papers in various international journals and presented 5 papers in international conferences. His research area is Digital Image Processing.

M.Arun., MCA., is working as an Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India. He has 9 years of teaching experience and published 7 papers and attended more than 6 international conferences. His research area is IoT, Mobile Computing.

R. Kalpana., MCA..M.Phil., is working as an Assistant Professor in Sri Krishna Adithya College of Arts and Science, Coimbatore, India. She has 4 years of teaching experience and published various research papers in peer reviewed journals. Her research area is Data Mining and Spatial Data Mining.



M.Athigopal, B.Ed.,M.Sc.,M.Phil., is working as an Assistant Professor in Subbalakshmi Lakshmipathy College of Science, Madurai, India. He presented 10 papers in national and international conferences and published 4 papers in international journals. His area of interest is IoT, Computer Networks.