Network Security System with Optimized Randomized Multiple Key Exchange Algorithm

Radhika.S, Chandrasekar. A, Jothi S, Jean Justus J

Abstract: ***This paper illustrates three different algorithms to provide shared secret key for security of the system. The proposed three algorithms namely 1) Modified Simple Password Key Exchange Scheme 2) Modified Diffie-Hellman Key exchange Scheme 3) Modified Elliptic Curve Scheme are meant to provide shared secret key for authentication process. Enhancements in terms of memory requirement, storage and other security properties such as authentication among mutual users, fraud prevention, attack etc., prove the validity of the proposed algorithms in proving authentication for the cryptographic identification of networks.***

Keywords: authentication, Diffie-Hellman, Secret key, Simple Key Exchange.

I. INTRODUCTION

Elliptic Curve Cryptography (ECC) finds its usage in various fields due to the lesser number of keys. The other advantages include higher speed, lesser memory requirement together with lesser power consumption and bandwidth. Due to this nature several countries and organizations have adopted ECC as their security mechanism. All cryptographic systems are evaluated by the strength of the algorithm that resists the attack. The ECC resists more than other algorithm in terms of more time that is required to break the algorithm. The Public-key schemes are generally used for keys exchange in symmetric-key ciphers. The strength of any public key system is evaluated in terms of the resistance level to break the symmetric keys. Table 1 illustrates NIST guidelines for selection of computationally equivalent symmetric and public key sizes.

Table1. Equivalent key size (in bits)

Symmetric	ECC	RSA/DH/DSA	MIPS Yrs to attack	Protection lifetime
80	160	1024	1012	Till 2010
112	224	2048	1024	Till 2030
128	256	3072	1028	Not till 2031
192	384	7680	1047	
256	512	15360	1066	

From the Table 1 it is evident that it is possible to provide complete security of symmetric algorithms only if the key size is made higher than 80 bits. Shamir A. and Tromer E (2003) insisted the urgent need to move to higher bit keys and they predicted that the changeover will take place at an earlier time than expected. Thus it is required to have a larger key size for longer protection level. Due to the performance enhancement of ECC over RSA is very high, ECC is found to be used widely and it becomes necessary.

The growth in the field of both personal and general communication systems has given rise to newer security threats. The threats can be the stealing of data or information and use them for illegal activities or it can be used to do fraud etc. Thus the channel meant communication should have security features such as confidentiality, intractability etc.

In a communication system, the users on both sides need to authenticate themselves and should share a secret key which will be used for further communication and other purposes like encryption. There are several literatures available. The one proposed by Beller M.J et al.,(1993) gives both side authentication and agreement of key with lesser computational complexity. The pre computation process is avoide by the protocol proposed by Aziz and Diffe (1994). These protocols make use of public key cryptography techniques. Also an off-line certification procedure is being followed.

The earlier versions of cryptography use secret key encryption for on-line certification of the users. Here the client and the server share a common secret key in prior. The public key cryptography makes use of separate key for both encryption and decryption. They also provide signature generation by digital signature methods. The above method suffer from long time delay during long message transfer. Thus in order to satisfy needs of the present digital communication system, high security ,less complexity ,power and less overhead is expected. The proposed protocol provides multiple key exchange, authentication, confidentiality and intrusion detection for digital communication systems.

Harn L. and Yang S. (1993) proposed a cryptographic scheme which is based on ID. Beller M.J., Chang L.-F. and Yacobi Y.(1993) described how to have privacy and authentication in portable communications. Ashar aziz and whitfield Diffie (1994) developed a protocol for wireless local area network. Refik Molva, Didier Samfat and Gene Tsudik (1994) developed another protocol named ‘Authentication protocol for mobile users’, which was published in the Institution of Electrical Engineers. Hugo Krawczyk (1996), introduced a

Revised Manuscript Received on January 05, 2020.

***** Correspondence Author

Radhika S, Department of Electrical and Electronics Engineering, School of Electrical and Electronics, Sathyabama Institute of Science and Technolgy,Chennai, India. .Email:radhikachandru79@gmail.com.

Chandrasekar A, Department of CSE, St.Joseph’s College of Engineering,Chennai,India. Email: drchandrucse@gmail.com

Jothi S. Department of CSE, St.Joseph’s College of Engineering,Chennai,India. Email: jothi14.baskar@gmail.com

Jean Justus J. Associate Professor **D**epartment of CSE, St. Joseph’s College of Engineering, Chennai, India. Email: jeanjraj@gmail.com

key exchange method for users of the internet. Hung-Yu Lin and Lein Harn (1995) proposed another security protocol which was 'Authentication protocols for personal communication systems', which says about the authentication for a personal computer and the work was published in Computer Communication Review. Chang-Seop Park (1997) published his work in Network IEEE in which he proposed a security protocols for wireless mobile communications.

Nassar Ikram (2001) discussed on how to identify users over network, and his work was published in IEEE as 'Cryptographic identification of users over network'. Yuebin Bai and Hidetsune (2003) discussed the detection of unauthorized person technology and development . Yuebin Bai and Hidetsune Kobayashi (2003) published their work in which they discussed about the network intrusion detection with string matching technology. Jean Justus and Chandrasekar (2016) elaborates on security issues in wireless sensor network. Dong Yu and Deborah Frincke (2004) published their work,an 'Towards Survivable Intrusion Detection System' in which they discussed the intrusion detection system which is survivable. Selvan M.P., Chandra Sekar A (2014) describes ranking of websites by its own features, whereas by Joseph Manoj R., Chandrasekar A .(2013,2014), an improved scheme for authorization of web services was explained. Edith J.J., Chandrasekar A.(2014) developed an architecture for detection of attacks using machine learning techniques. Haoyu Song and John W. Lockwood (2005), proposed a work on Network Intrusion Detection Systems in which they discussed about unauthorized intruder detection Systems. Rajesh S., Chandrasekar A (2016) proposed a design model using prioritization. Jianming Yu and Yibo Xue (2006), proposed an algorithm for network security. Chandrasekar etal (2011) discussed on secured key using 512 bit.

The Diffie-Hellman key exchange is the first public key algorithm. The algorithm suffers with the following limitations.

- Brute-force attack is possible by knowing Prime number (q), primitive root (α), public key of A and B and the secret key K can be computed.
- Reply attacks.

Elliptic Curve Diffie-Hellman (ECDH) Key Exchange protocol provides a shared key between client and server . The Limitations are:

- Possibility for Brute-force attack will be reduced but we cannot say it is fully removed.
- Reply attacks.
- The Public key of both the User and Server are not protected.
- For every transaction both the server and user should be initiated repeatedly

This protocol consists of three parts.

- Generation of Key.
- Generation of Signature.
- Verification of Signature.

The purpose of key generation is used to generate Public and Private Key of the users. The purpose of signature generation is to generate signature for the message using Secure Hash algorithm. The purpose of signature verification is to verify A's Signature by user B and to accept or reject the message. The limitations of ECDSA are

- Used only for Authentication.
- Key agreement should be done separately before authentication.
- For every transaction both the Key agreement process & Authentication should be repeated.
- Suitable only for a Home network.

Limitations of Existing Protocols

- Brute-force attack is possible in all existing protocols.
- Reply attacks are also possible in all existing protocols.
- The public keys of both are not protected.
- Key agreement and authentication should be done separately.
- For every transaction both the Key agreement & Authentication process should be repeated.
- The existing technology encodes the bits using elliptic curve exponent key exchange.
- The curve is defined over Galois field and share a public key at the receivers end.
- Using this key the receiver encodes the data and does reply to the sender.
- Existing system works fine until the algorithm used remains undiscovered.
- Once there is leak in the encryption algorithm it helps the hacker to identify the patterns quite easily, hackers can decode the data being sent.

II. RANDOMIZED KEY-EXCHANGE METHOD SELECTION

The randomized key-exchange method selection is based on the random number selection. A random number for 0 to 65535 will be generated; selected random number will be divided by the numeral three. The reminder of the division (modulo operation) will be used to select the algorithm. If remainder value is 0, Modified Diffe-Hellman Algorithm will be selected, if remainder value is 1, Modified Simple password key exchange will be selected, if remainder value is 2, Modified Elliptic Curve will be selected. Figure 1, shows how randomized key exchange method selection is working

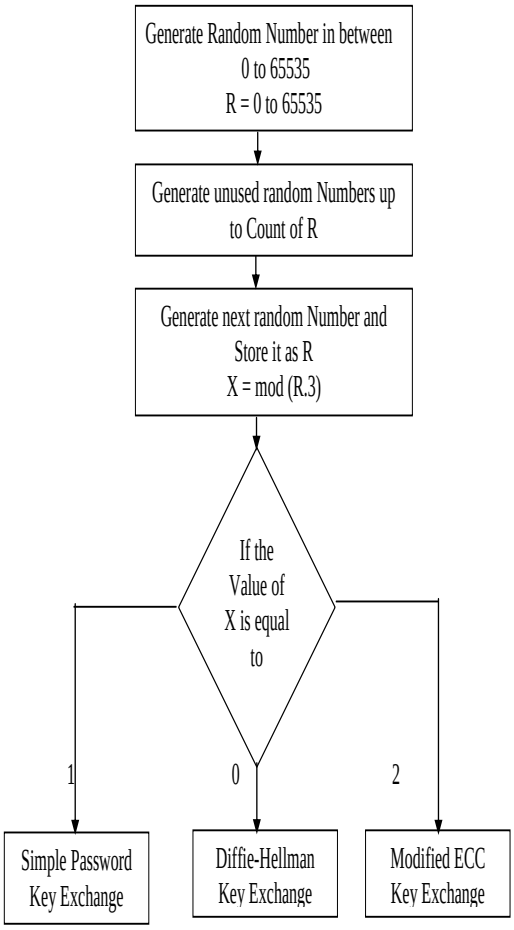

Figure 1 Randomized key exchange method selection

.

A. *Modified Diffie-Hellman Key Exchange Scheme*

The work is to make two users to exchange a key secretly which can be used for message encryption. This algorithm has the following: There are two numbers which are known publicly, one is a prime number 'q'. The other one is an integer 'a' that is a primitive root of 'q'. These two numbers are common to all users by using Diffie-Hellman scheme. It should be noted that mod "q" is generated by using power of 'a'. The two users A and B selects x's random keys and by using exponentiation, they generate public y's to protect x's. An intruder who knows y's exchange is required to solve a discrete logarithmic problem to obtain x's which is computationally hard.

Figure 2, shows how exchange takes place in the Modified Diffie-Hellman key exchange scheme. The actual key exchange for either party consists of generating private keys using public key. The key for the block cipher or other private key scheme is the obtained number. An attacker who wants to obtain the same value needs at least one of the secret numbers, which implies ,it has solve a hard problem which is function logarithmic. It should be noted that if A and B finally make communication, the same key is retained as such, unless they choose new public-keys.

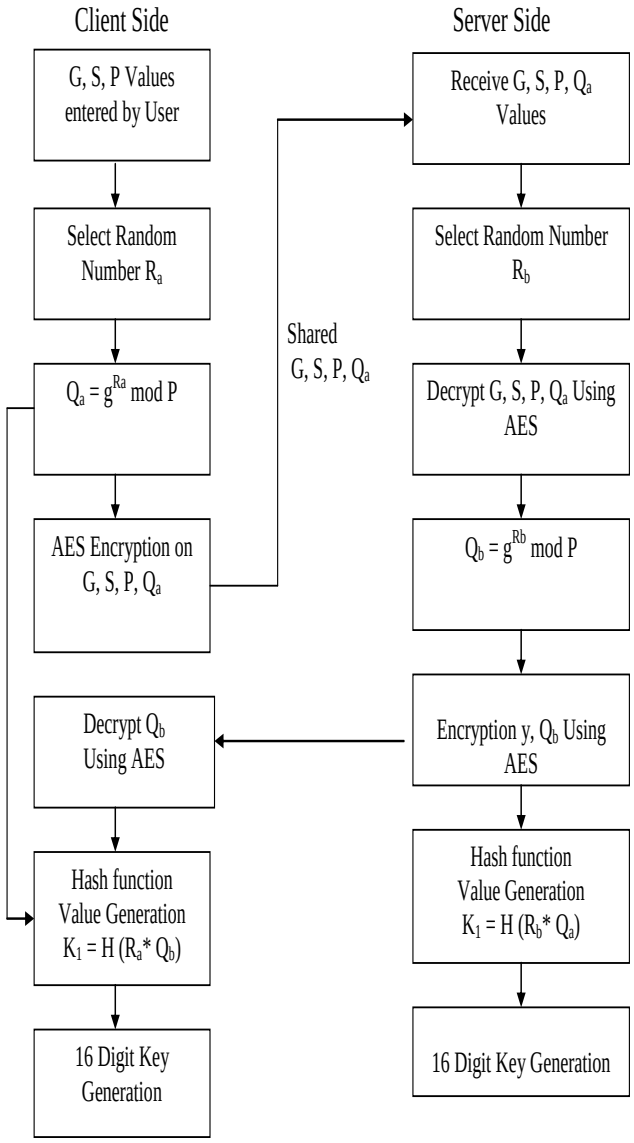

Figure 2 Modified Diffie-Hellman Key Exchange

B. *Modified Simple Password Key Exchange*

A new temporary public key pair is generated by 'A'. The public key is send by 'A' to 'B' along with their identity. The session key 'K' is generated by 'B' and is send to 'A' after being encrypted by using the supplied public key. The session key is decrypted by 'A' and both (A & B) uses the public key. The problem that exists is that an opponent can intercept and impersonate both halves of protocol. The Figure 3 shows the modified simple password key exchange, which provides authentication & key establishment over an insecure channel. The modified scheme closely related to Modified Diffie-Hellman key exchange scheme. But both are different in their constructions.

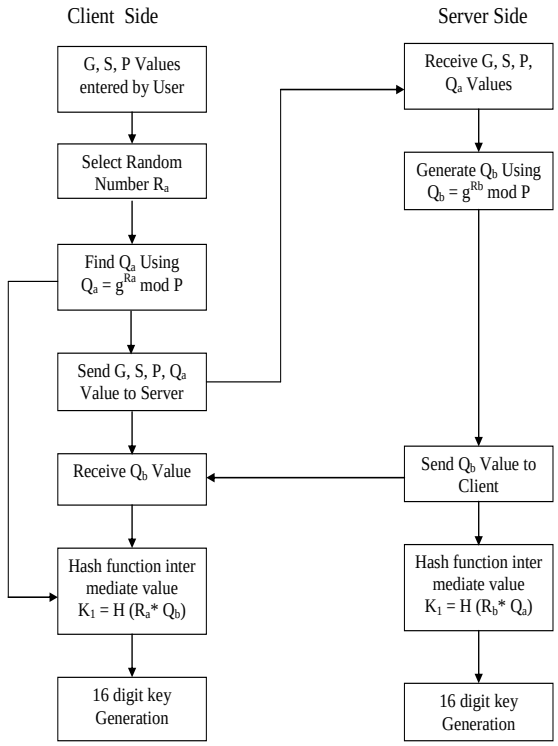

Figure 3 Modified Simple Password Key Exchange

C. *Modified Elliptic Curve Key Exchange*

A major concern with the public key cryptography is the size of the numbers being used as it decides the storage requirement. The earlier system uses integer or polynomial arithmetic whereas the existing ECC uses elliptic curve arithmetic. ECC uses the equation $y^2 + ay = x^3 + bx + c$ where a, b, c ∈ F , q, $a \neq 0$. In existing ECC, a fixed key is used to encrypt the Q value. In modified ECC, for key generation, a polynomial based inner-level-key-exchange is used. This key is used for encryption of the Q value.

1) Polynomial based sub key generation

Two polynomials gu(x), hu(y) are used. They are obtained as the product of z = f(x, y) intersection with planes y = u and x = u where z is the surface.

$gu(x) = f(x, y)|y=u$ (1)

$hu(y) = f(x, y)|x=u$ (2)

Degrees of those polynomials are equal. Two nodes u1 and u2 get pair of polynomials gu1 (x), hu1 (y) and gu2 (x), hu2 (y) that intersecting exactly two points:

gu1 (u2) = f(u2, u1) = hu2 (u1) (3)

hu1 (u2) = f(u1, u2) = gu2 (u1) (4)

The Figure 4 shows the modified Elliptic Curve Cryptography key exchange, in which polynomial based sub key generation is used.

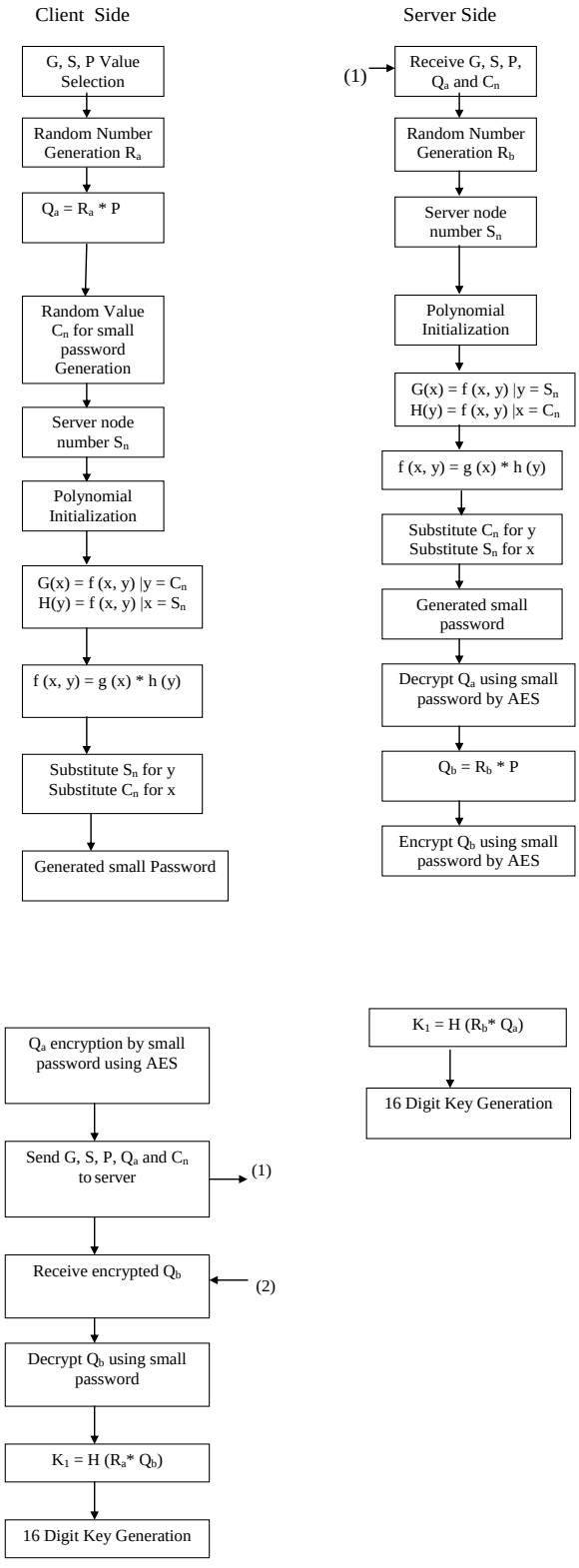

Figure 4 Modified Elliptic Curve Key exchange

III. RESULT AND DISCUSSION

The result of the proposed system was compared with certain properties of the existing protocols.

Security properties

Security properties were compared with stste of art protocols and is summarized in Table 2.

Table 2 Security Properties Comparison with existing protocols

Items of Security	Jian Wang et l(2007)	Proposed Protocol
Mutual authentication	Yes	Yes
Prevention of fraud	Yes	Yes
Prevention of replaying attack	Partially	Fully
Message integrity	available	available
Anonymity	available	available
Renewal of Key	Yes	Not available
Secure dynamic participation	available	available

For a particular session. The above table shows that the proposed protocol provides a complete prevention of replaying attack and key renewal must be done only once for a session.

Bandwidth Table 3 shows the comparison of total number of exchanged bits (Bandwidth required) in existing protocols with the proposed one. Figure 5 shows the graphical comparison of bandwidth required for the proposed protocol with the existing protocols. It is evident from Figure 5 that the proposed one is lesser in the bandwidth requirement than the existing ones.

Table 3 Bandwidth comparison with existing protocols

Protocol	Bits exchanged
Beller-Chang-Yacobi	8320 bits
Aziz-Diffie	8680 bits
Proposed	6510 bits

Memory Utilization

Memory consumption by the proposed system is also less while comparing with the existing security protocols. Figure 6 shows the comparison of the memory requirement with the state of art protocols. Thus from the Figure 6, it can also claim for lesser storage space from the user point of view.

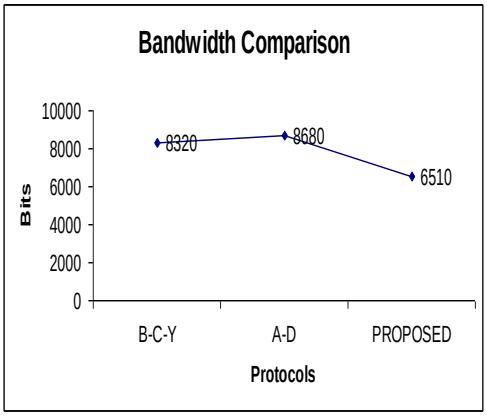

Figure 5 Bandwidth comparison

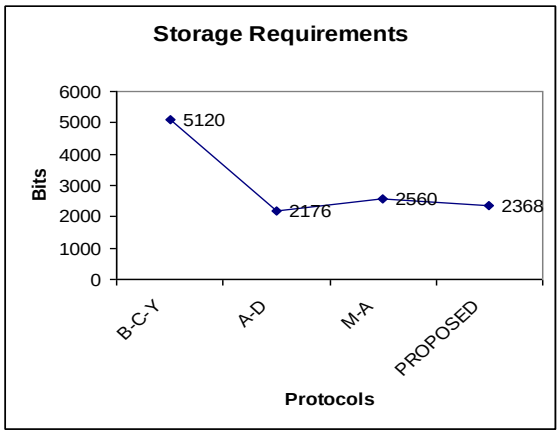

Figure 6 Storage requirements

Accuracy

The use of Advanced Encryption Standard encryption makes sure that the encryption and decryption takes place without any errors or loss of data. Hence the accuracy is high and reliable in encrypting the data.

Faster Processing

Due to the use of simple algorithms and mathematical calculations it is seen that maximum security is maintained without compromising the efficiency or runtime.

IV. CONCLUSION

In this paper, three optimized secret key exchange algorithms are proposed. This proposed system, when comes to real practice will provide us with a much more improved security system. Moreover the proposed system will be a new challenge for the hackers who attack the system. Multilayer security makes the communication more secured and less vulnerable. This work would be of great use for securing the critical data in Government and private sectors.

Future enhancements are concerned, a new random number generation algorithm will be developed, which will encrypt the random number while transfer. The proposed algorithm will be extended to use in wireless networks and handheld devices. The proposed system will be further enhanced to be used for online transactions. Biometric security methods can be used in addition with the proposed system. The system can be extended to use with ad-hoc networks also. In new string match based NIDS, instead of single Next Array a two dimensional Next Array can be used, which makes the intrusion detection faster and accurate.

REFERENCES

1. Ashar aziz and whitfield Diffie.(1994), 'A secure communications protocol to prevent unauthorized access: Privacy and authentication for wireless local area networks', IEEE Personal Communications, pp. 25-31.
2. Beller M.J., Chang Li.-Fung. and Yacobi Y. (1993), 'Privacy and authentication on a portable communications systems', IEEE Journal on Selected Areas in Communications. VOL. 11, NO. 6, pp 821-829
3. Chang-Seop Park (1997), 'On Certificate Based Security Protocols for Wireless Mobile Communication Systems', IEEE Network, pp 50-57.
4. Chin-Chen Chang and Shih-Chang Chang (2008), 'An Improved Authentication Key Agreement Protocol Based on Elliptic Curve for Wireless Mobile Networks', IEEE, pp 1375-1378.
5. Diffie W. and Hellman M.E. (1976), 'New Directions in

Cryptography', IEEE Transactions on Information Theory, VOL.IT-22, NO. 6, pp. 644-654.
6. Dong Yu and Deborah Frincke (2004), 'Towards Survivable Intrusion Detection System', IEEE, pp 1-10.
7. Edith J.J., Chandrasekar A.(2014) Layered Architecture to Detect Attacks Using Asymmetric Support Vector Machine, Journal of Applied Security Research,9(2), pp. 133-149
8. Haoyu Song and John.W Lockwood (2005), 'Multi-pattern Signature Matching for Hardware Network Intrusion Detection Systems', IEEE, pp 1686-1690.
9. Harn L. and Yang S. (1993), 'ID-Based Cryptographic Schemes for user Identification, Digital Signature, and Key Distribution', IEEE Journal on Selected Areas in Communication, Vol. II, No. 5, pp. 757-760.
10. Hugo Krawczyk (1996), 'A Versatile key exchange mechanism for internet ',IEEE,pp 114-127.
11. Hung-Yu Lin and Lein Harn (1995), 'Authentication Protocols for Personal Communication Systems',ACM,pp 256-261.
12. Jean Justus J., Chandra Sekar A.,(2013) A fault tolerance data aggregation scheme for wireless sensor networks, International Review on Computers and Software,8(7), pp. 1556-1563
13. Jian Wang, Nan Jiang, Hui Li, Xinxin Niu and Yixian Yang (2007), 'A Simple Authentication and Key Distribution Protocol in Wireless Mobile Networks', IEEE, pp 2282-2285.
14. Jianming Yu and Yibo Xue(2006) , 'Robust Quick String Matching Algorithm for Network security', International Journal of Computer Science and Network Security, Vol.6 No.7B, pp 180-184.
15. Jianxiao Liu and Lijuan Li (2008), 'A Distributed Intrusion Detection System Based on Agents', IEEE, pp 553-557.
16. Joseph Manoj R., Chandrasekar A.(2014), An enhanced trust authorization based web services access control model, Journal of Theoretical and Applied Information Technology, 64(2), pp. 522-530
17. Joseph Manoj R., Chandrasekhar A. (2013), An authentication system of web services based on web server log analysis, International Journal of Engineering and Technology,5(6), pp. 4786-4793.
18. Justus J.J., Sekar A.C. (2016), Energy efficient priority packet scheduling with delay and loss constraints for wireless sensor networks, International Conference on Inventive Computation Technologies, ICICT 2016.
19. Kun Huang and Dafang Zhang (2008), 'A Byte-Filtered String Matching Algorithm for Fast Deep Packet Inspection', IEEE Computer Society, pp 2073 – 2078.
20. Nassar Ikram (2001), 'Cryptographic identification of users over network', IEEE, pp 59-63.
21. Rajesh S., Chandrasekar A.(2016) An efficient object oriented design model: By measuring and prioritizing the design metrics of UML class diagram with preeminent quality attributes, Indian Journal of Science and Technology,9(21).
22. Molva, Refik, Didier Samfat, and Gene Tsudik. "Authentication of mobile users." *IEEE Network* 8.2 (1994): 26-34.
23. Sekar A.C., Radhika S., Anand K.,(2011), "Secure communication using 512 bit key", European Journal of Scientific Research, 51(1), pp. 61-65
24. Selvan M.P., Chandra Sekar A(2014).Ranking websites by its own features, International Journal of Applied Engineering Research,9(22), pp. 12049-12056.
25. Shamir A. and Tromer E. (2003), 'Factoring Large Numbers with the TWIRL Device', LNCS 2729, Springer-Verlag, pp 1-26.
26. U.S. Dept of Commerce/NIST (2000), 'Digital Signature Standard (DSS)', FIPS PUB 186-2, pp 1-70.
27. Yuebin Bai and Hidetsune (2003), 'Intrusion detection systems: Technology and development', IEEE Computer Society.
28. Yuebin Bai and Hidetsune Kobayashi (2003), 'New string matching technology for network security', IEEE Computer Society.
29. Zhang Hu (2009), 'Design of Intrusion Detection System Based on a New Pattern Matching', IEEE, pp 545-548.

AUTHORS PROFILE

Dr.S.Radhika is a professor from School of Electrical and Electronics Engineering of Sathyabama Institute of Science and Technology since 2006. She completed her Ph.D with research title "Design of Adaptive Filtering Algorithms for Acoustic Echo Cancellation Application. Her areas of research include *Adaptive signal processing, system identification, echo cancellation and sparse signal processing.* She has published several articles in international and national journals and conferences related to the adaptive filter algorithms.

Dr. A. Chandrasekar is Professor and Head of the Department of CSE at St. Joseph"s College of Engineering, Chennai, Tamil Nadu. He has overall teaching experience of over 21 years in Engineering Colleges. He has guided more than 12 Research Scholars and more than 50 M.E. students. He has published over 110 research articles in refereed International and National journals and he is guiding research scholars and M.E. students in the areas of Network Security, Cloud Security, Data mining, Artificial Intelligence and Big Data Analysis.

Dr. S. Jothi is Associate Professor of the Department of CSE at St. Joseph"s College of Engineering, Chennai, Tamil Nadu. She has completed her Bachelor of Engineering Degree in Computer Science and Engineering from Madurai Kamaraj University in the year of 2003. She has completed her Master of Engineering in Computer Science and Engineering from Annamalai University in the year of 2005. She has completed her Ph.D. in Wireless sensor networks from Anna University, Chennai, in the year of 2016. She has published 12 technical papers in various journals. She has 13 years of teaching experience on graduate and post-graduate level. Her area of interest includes Wireless Sensor Networks, Mobile ad-hoc Networks, Big Data Analysis and Image Processing.

Dr. J Jean Justus is Associate Professor of the Department of CSE at St. Joseph"s College of Engineering, Chennai, Tamil Nadu. She has completed her Bachelor of Engineering Degree in Computer Science and Engineering from Manonmanium Sundaranar University in the year of 2001. She has completed her Master of Engineering in Computer Science and Engineering from SastraUniversity in the year of 2004. She has completed her Ph.D. in Wireless sensor networks from Anna University, Chennai, in the year of 2017. She has published 10 technical papers in various journals. She has 15 years of teaching experience on graduate and post-graduate level. Her area of interest includes Wireless Sensor Networks, Mobile ad-hoc Networks, Big Data Analysis and Image Processing.