IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Special Issue 2, December 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

An Efficient Secure Dynamic Authentication for WSN Using Dynamic Salt Approach

Dr. D.J.Evanjaline[1], V. Elamurugu[2]

Asst.Professor, Department of Compute, Rajah Serfoji Govt Arts and Science College, Thanjavur, India[1]

Research Scholar, Department of Compute, Rajah Serfoji Govt Arts and Science College, Thanjavur, India[2]

ABSTRACT: Wireless of security threats. To overcome this issue, secure communication is necessary between network entities. Authentication is one of the protections against unauthorized access, illegal eavesdropping, and tampering insecure transmission. This paper proposes an efficient, secure dynamic authentication for WSN using a dynamic salt algorithm. In cryptography Sensor Network (WSN) comprises a huge number of resource-constrained sensor nodes used in communications systems and remote monitoring in industries like healthcare services, security, farming, and disaster risk management. Due to the increasing utilization of wireless sensor networks, critical information is shared in an insecure channel among networked devices such as sensors, gateways, users, etc. The existence of essential and sensitive data in the network raises the significance, a salt is a random string attached to the prefix or postfix of the original user's password before it is entered into a hash function. For WSN protection, adding Salt as a prefix or postfix to the original text is insufficient. There are several methods for recovering the original text from the ciphertext. This paper proposes an efficient improved salt password hashing method based on the dynamic key approach. This proposed work uses a simple hashing algorithm with very low time complexity as most of the steps involved simple binary XoR operations and is well suited for WSN.

KEYWORDS: Authentication, dynamic encryption, hash function, salt algorithm

I. INTRODUCTION

With advanced developments in ubiquitous computing, Wireless Sensor Network (WSN) will become the next generation network. It comprises a group of sensor nodes distributed at random to communicate through the wireless channel to track environmental parameters such as sound, friction, strain, weather, and so on. The WSN is composed of three main components [1]: a gateway node (GW), a sensor node (SN), and a user (U). The sensor node monitors the physical environment, and GW facilitates communication between the user and the sensor node. Sensor nodes collect useful data, which are capable of computation but have limited storage space. The information gathered by the gateway is accessible to users. The data communication in a WSN is shown in Figure 1.

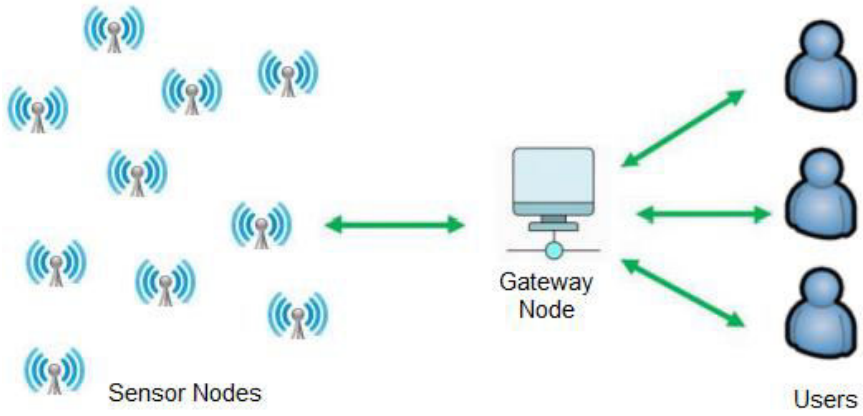

Figure 1 Generalized Communication Model of WSN

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

The sensor nodes are typically battery-powered, WSN protocols and frameworks are designed to use energy as efficiently as possible to extend the network lifetime. Due to the computationally intensive nature of security algorithms, most WSN applications may not even consider security requirements. As the network is tracking and exchanging sensitive data, protection becomes a major concern that must be addressed. Even if the data being transmitted is not sensitive, it is important to verify the validity of the neighbour to whom the information is being sent, and the recipient must be assured that the data has not been tampered with (data integrity). Data privacy, data integrity, authentication, non-repudiation, and compatibility are only a few of the security requirements for a wireless network [2]. The network may not meet all of the specifications; requirements may vary depending on the application.

An authentication protocol is a widely used security mechanism [3] that creates a session key for communication parties to achieve safe data transfer. It's not easy to come up with a realistic authentication protocol for resource-constrained WSNs. The efficiency of hash function-based techniques is high, but the protection of the session key is difficult to ensure. Many WSN authentication schemes [4][5], including hash function and public key cryptosystem-based schemes, have design flaws and are vulnerable to various security threats, such as forgery and replay attacks, and fail to provide user anonymity among other things. Designing an authentication protocol for WSNs that ensures protection while remaining cost-effective becomes a difficult challenge.

This paper proposes an efficient and secure dynamic authentication for WSN using the dynamic salt approach. This method combines dynamic Salt with a hash-based password technique. Dictionary and brute force attacks for cracking several passwords are made even more difficult by the random salt string. The advantage of the Salt is that if multiple people use the same password, the attacker will not be aided because the Salt will append a random string to the identical passwords.

The rest of the paper is organized as follows: Section 2 reviews various authentication schemes in WSN and different salt algorithms. The preliminary concepts are described in section 3. The proposed dynamic Salt-based authentication scheme is explained in section 4, and Section 5 analyzes the performance of the proposed work. Finally, section 6 concluded the paper.

II. RELATED WORK

This section describes the various authentication schemes for WSN, dynamic key management in WSN and different Salt-based techniques to secure passwords.

Jung [6] suggested a lightweight authentication scheme based on three-factor authentication and a key agreement protocol. This method utilizes XOR and hash function to resolve several security concerns. Based on the hyper elliptic curve Diffie-Hellman, Naresh [7] presented a novel multiple shared key agreement for WSN. The protocol reduces key exchange overhead while also increasing key security. González et al. [8] introduced a lightweight password-authenticated key exchange for heterogeneous WSN. It examines three-party key exchange protocols with password authentication. This protocol provides privacy-preserving, adaptable, and effective security features.

For heterogeneous WSN, Athmani et al. [9] propose an efficient dynamic authentication and key management scheme. Although maximizing the protection level, this approach offers a single lightweight protocol for authentication and key establishment. The key distribution method creates dynamic keys using preexisting information and does not need a secure channel or sharing process, which improves protection, energy efficiency, and memory usage. Lee et al. [10] developed a three-factor authentication protocol for WSNs that excludes ECC and uses the fuzzy-extractor for biometric knowledge. This proposal employs the honey list strategy to counter malicious attacks such as smartcard theft and simultaneous identity and password guessing.

S. Mesmoudi et al. [11] designed a smart and dynamic key management scheme for hierarchical wireless sensor networks. The method involves key development, key renewal, and the addition of new nodes. This protocol uses machine learning to monitor network activity and select the required level of protection. During various phases, the number and size of messages exchanged remain high. Yousefpoor and Barati [12] developed an intelligent dynamic key management system that uses fuzzy logic for path key generation and adding new nodes to the network. It employs both pre-distribution and post-deployment key distribution mechanisms among sensor nodes.

A dynamic key generation strategy is proposed in [13] that combines a pre-shared/stored secret key with a variable nonce derived from channel information. The main advantage of this method is that it provides high security with minimal overhead. A preamble encryption algorithm is also proposed to prevent unauthorized synchronization or channel measurement by invalid users. The proposed cipher scheme's security level is primarily determined by the secret key and the dynamicity of the channel used to modify the cipher primitives for each frame symbol.

One of the most effective ways to secure user passwords is to use the salted password hashing technique. Karrar et al. [14] suggested salted password hashing methods based on an array algorithm swapping elements. This method uses two

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

key processes: hash input rearrangement and salt rearrangement, aiming to improve the salted password hashing technique by rearranging hash input before hashing it and scrambling Salt before storing it in the database.

Bachtiar et al. [15] address data protection using dynamic encryption and use a modified version of the AES 256-bit algorithm. By adding a word (Salt) to plain text, a procedure is generated to produce dynamic encryption. A Linear Congruential Generator (LCG) algorithm resulted in the formation of Salt. Then, using the One Time Pad algorithm (OTP), a mixture of Salt and plain text will be combined.

Sutriman and B. Sugiantoro [16] explore how to increase the security of hash algorithms by using a combination mechanism other than the prefix and postfix between password and Salt. Jeong et al. [17] proposed an access log based salt method. Salts dependent on access are constantly changing, allowing passwords more secure while still concealing Salt's identity. Ali et al. [18] proposed encrypting iterative salted hashes called anti-continuous collision salted hash encryption, which employs cryptography to generate a stable pseudo-random number generator, which is then hashed with password data using a secure hashing algorithm.

A new password-based authentication scheme is presented by Chowdhury et al. [19]. Intermixing a fixed text (a traditional part of a password) with a free arbitrary text (newly added) at various pre-defined indexes of different pre-defined lengths is the basis of this scheme. The inclusion of the free random text increases the complexity of cracking the password.

1. PRELIMINARIES

Hash Function

Hash function (h(·)) is an algorithm that encodes messages into a fixed digits digital signature, such that it is infeasible to derive the original message from the encoded digits.

A one-way hash function is defined to be secure if the following properties can be achieved: [20]

- Input a message x of arbitrary length, and it is easy to compute a message digest of a fixed-length output h(x).
- Given y, it isn't easy to compute $x = h^{-1}(y)$.
- Given x, it is computationally infeasible to find x 0 6= x such that h(x') = h(x) holds.

To produce the appropriate hash values of the password, cryptographic hashing functions are used. To determine the hash value, these functions use a variation of transposition techniques and XoR operations each time. For example, the MD5 hash function return hash value for the word 'secret' is 5ebe2294ecd0e0f08eab7690d2a6ee69 and the SHA-1 generate e5e9fa1ba31ecd1ae84f75caaa474f3a663f5f4.

Salt

Salt [17] is a random string of characters, numeric digits, or special characters appended to a password so that the hash values maintain maximum randomness after hashing. In database storage systems, it's best to use unique salt values for each password. Salt is added to the string does not assure complete secrecy, but it does ensure that cracking the password is computationally impossible. The strength of salted hash values may be that even brute force attacks would take a long time to decrypt the hash. Since salts are private, using two salts, one public and one private, will protect a password from offline password guessing attacks. [18].

To create a Salt Hash password, follow these steps:

- Obtain a password; (secret)
- Create Salt using reliable arbitrary methods (3df6)
- Add salt string to the obtained password. (secret3df6)
- Using the required hash function, create a Salt Hash password (1475d56e4aa8158c27d5da154a10601f757073).
- Save the Salt and the salt hash to the database.

III. METHODOLOGY

Due to their unsecured and violent deployment in the field, user authentication is a critical security issue in wireless sensor networks. Authenticating remote users in such a resource-constrained setting is a major security problem, given that the sensor nodes are equipped with limited processing power, memory, and communication devices. The use of lightweight cryptographic primitives like symmetric key encryption/decryption and hash functions to design user-anonymous authentication schemes was impressive.

This section proposes a secure and efficient authentication scheme for WSN using a dynamic salt approach. The proposed method contains three phases: Registration, Authentication and Password change. Table 1 shows the notations used in this paper.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Table 1 Notations and Meanings

Entity	Notation	Meaning
User	U_i	i^{th} User
	U^{ID}_i	User Identity
	U^{PWD}_i	User Password
	U^{PIN}_i	User PIN
	U^{S}_i	User Salt value
	U^{PWDSH}_i	User Password Salt Hash value
	U^{PINSH}_i	User PIN Salt Hash value
	U^{ECP}_i	User Encrypted Password
Sensor	SN_j	j^{th} Sensor Node
	S^{ID}_j	Identity of j^{th} Sensor Node
	S^{S}_j	Sensor Salt value
	S^{SH}_i	Sensor Salt Hash value
Operator	h(.)	Hash Function
	bin(.)	String to Binary Conversion
	‖	String concatenation
	⊕	Exclusive-Or

A. Registration Phase

To access WSNs service, a user U_i and a sensor S_j have to register with gateway GWN.

User Registration

User U_i selects unique identity U^{ID}_i, password U^{PWD}_i, PIN U^{PIN}_i and generate a random salt value (U^{S}_i), then compute the following values to register with the GWN. This paper creates a salt value based on the combination of random numbers and characters (alphabets lowercase and uppercase) with 8-bit length. The detailed steps involved in a user registration process as follows:

User Registration with GWN
1: User U_i select User Identity U^{ID}_i , Password U^{PWD}_i and Pin Number U^{PIN}_i
2: Generate random salt value (U^{S}_i)
3: If U^{PIN}_i % 2 ==0
4: V1=append (U^{S}_i) with U^{PWD}_i in even position
5: V2 = append (U^{S}_i) with U^{PIN}_i in odd position
6: Else
7: V1= append (U^{S}_i) with U^{PWD}_i in odd position
8: V2 = append (U^{S}_i) with U^{PIN}_i in even position
9: EndIF
10: U^{PWDSH}_i = h(V1) and U^{PINSH}_i = h(V2)
11: V3 = h(U^{ID}_i ‖ V1) and V4 = h(U^{ID}_i ‖ V2)
12: U^{ECP}_i = h(U^{PWDSH}_i ‖ U^{PINSH}_i) h(V3 ‖ V4)
13: User U_i send U^{ID}_i , U^{S}_i and U^{ECP}_i to GWN
14: If U^{ID}_i already exists in GWN then
15: Send a denial notification to U_i
16: Else
17: GWN store U_i information [U^{ID}_i , U^{S}_i and U^{ECP}_i]
18: End If

Sensor Registration

This subsection explains sensor registration with the gateway node. Each sensor node is configured with unique S^{ID}_j when the time of node deployment. The following step describes the sensor registration.

Sensor Registration with GWN
1: Sensor SN_j select S^{ID}_j
2: Generate random salt value (S^{S}_i)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

3: Compute $S^{SH}_j = h(S^S_j)$
4: $X1 = bin(S^{ID}_j) \oplus S^{SH}_j$
5: Sensor Node SN_j send X1 and S^{SH}_j to GWN
6: GWN Compute $X2 = X1 \oplus S^{SH}_j$
7: $X3 = h(X2 \| S^{SH}_j)$
8: GWN store X2 and X3 and send X3 to SN_j

B. Authentication Phase

The user login process is used to verify the user's credentials, prevent a denial of service attack and access the sensor node gathered information. The user computes the authentication information and then compares it to the previously stored data. After authentication, the legitimate user is granted access. The following steps are used to authenticate user U_i

User Authentication
1: User U_i provide U^{ID}_i, U^{PWD}_i, U^{PIN}_i and get U^S_i
2: Compute V1 and V2 based on U^{PIN}_i
3: Compute $U^{PWDSH}_i = h(V1)$ and $U^{PINSH}_i = h(V2)$
4: $V3 = h(U^{ID}_i \| V1)$ and $V4 = h(U^{ID}_i \| V2)$
5: $newU^{ECP}_i = h(U^{PWDSH}_i \| U^{PINSH}_i) \oplus h(V3 \| V4)$
6: User U_i send $newU^{ECP}_i$ to GWN
7: GWN retrieve U_i encrypted password U^{ECP}_i
8: If $newU^{ECP}_i == U^{ECP}_i$ then
9: Legitimate User access sensor information
10: Else
11: Illegal User request
12: End If

C. Password Change Phase

The following steps are used to modify the password U^{PWD}_i or PIN U^{PIN}_i of the User U_i.

Change Password
1: User U_i perform authentication process for User legitimate verification
2: User U_i retrieve salt value U^S_i
3: U_i input new password $newU^{PWD}_i$ and/or new pin number $newU^{PIN}_i$
4: Compute newV1 and newV2 based on $newU^{PIN}_i$
5: Recompute $newU^{PWDSH}_i$ and $newU^{PINSH}_i$
6: Recompute newV3 and newV4
7: Compute $newU^{ECP}_i = h(newU^{PWDSH}_i \| newU^{PINSH}_i) \oplus h(newV3 \| newV4)$
8: User U_i send $newU^{ECP}_i$ to GWN
9: GWN update U_i new password $newU^{ECP}_i$

IV. EXPERIMENTAL RESULTS

This section explains the performance evaluation of the proposed approach. The proposed dynamic authentication is simulated using Java (version 1.8), and the experiments are performed on an Intel(R) Pentium(R) processor with a speed of 2.30 GHz and 4.0 GB RAM using Windows 10 64-bit Operating System.

This section first shows how the user is registered with GWN
If the user U_i input
User Identity U^{ID}_i = 'LeeWang'
Password U^{PWD}_i = 'mysecret'
Pin Number U^{PIN}_i = 257
Randomly generated salt value of user U_i = 'aaUD30Hy'
The salt value can be generated based on the combination of numbers (0-9) and alphabets (a-z and A-Z).

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Salt Value Generation

```
String base = "0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz";
int saltsize=8;
Random random = new Random();
StringBuilder b = new StringBuilder();
for(int i = 0; i < saltsize; i++)
{
    b.append(base.charAt(random.nextInt(base.length())));
}
String saltvalue= b.toString();
```

Find the remainder value of PIN U^{PIN}_i. The remainder value is zero appends (U^S_i) with U^{PWD}_i in even position and appends (U^S_i) with U^{PIN}_i in odd place otherwise append (U^S_i) with U^{PWD}_i in an odd part and append (U^S_i) with U^{PIN}_i in even position.

The remainder value of U^{PIN}_i (257) is not equal to zero.

Salt Value

a	A	U	D	3	0	H	Y

Password

m	Y	s	e	c	r	e	t

Salt Password (salt in odd position)

a	m	a	y	U	s	D	e	3	c	0	r	H	e	Y	t

V1=amayUsDe3c0rHeYt

Salt Pin (salt in even position)

2	a	5	a	7	U	D	3	0	H	Y

V2=2a5a7UD30HY

The hash value is generated using the MD5 algorithm

Hash Value Generation

```
String v=" amayUsDe3c0rHeYt";
Byte data[]=v.getBytes();
MessageDigest md = MessageDigest.getInstance("MD5");
md.update(data);
byte[] bt = md.digest();
String hexString ="";
for (int i=0; i < bt.length; i++) {
        hexString +=Integer.toString(( bt[i] & 0xff ) + 0x100, 16).substring( 1 ).trim();
    }
```

U^{PWDSH}_i = h(V1) = 3ba867a11f65493ca427103bd20a7875

U^{PINSH}_i = h(V2) = f7d701f3e42431374fb7c6be66130255

V3 = h($^{UID}_i$ || V1) = h(LeeWang3ba867a11f65493ca427103bd20a7875)
= 1df36c2abc762ca4401d3089824889ea

V4 = h($^{UID}_i$ || V2) = h(LeeWang f7d701f3e42431374fb7c6be66130255)
= 47a768df57960f45f1b611da143cefd6

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

$U^{ECP}_i = h(U^{PWDSH}_i \| U^{PINSH}_i) \oplus h(V3 \| V4)$
= bin(dc49fa1c2c522a1807d7bbda07a9784b) ⊕
bin(afc5a69e9cc44512fe7e64b6c9f72760)

XoR Operation

String xor="";
StringBuilder sb = new StringBuilder();
for (int i = 0; i < s1.length(); i++)
sb.append(charOf(bitOf(s1.charAt(i)) ^ bitOf(s2.charAt(i))));
xor=sb.toString();

static boolean bitOf(char in)
{
return (in == '1');
}
static char charOf(boolean in)
{
return (in) ? '1' : '0';
}

The encrypted password is
=01110011100011000101110010000010101100001001011001101111000010101111100110101001110111111011100110011100101111001011111001010111

Salt Size in bits	Salt Generation Time (ms)	Time taken MD5 (ms)	Time taken SHA-1 (ms)
8	1	15	16
16	1	16	16
32	1	18	21
64	1	16	18
128	1	21	21
256	4	22	23
512	8	20	20

V. CONCLUSION

The number of sensors linked to real-world objects has increased as the Internet has grown. As a result, it is important to provide a secure WSN service that connects object sensors. This paper proposes a WSN authentication scheme that is efficient and reliable to ensure the validity and reliability of communication between the user-gateway and the sensor-gateway using a dynamic Salt-based technique. To achieve secure authentication, this paper uses a hash function, dynamic key generation and salt algorithm. The performance of the proposed method was analyzed, which proves that the proposed authentication scheme is lightweight and secure.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.569| || Volume 10, Special Issue 2, December 2021 ||

4th International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM '2021]

15th & 16th September 2021

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

REFERENCES

[1] M.F. Moghadam, M. Nikooghadam, MABA Jabban, M. Alishahi, L. Mortazavi and A. Mohajerzadeh, "An Efficient Authentication and Key Agreement Scheme Based on ECDH for Wireless Sensor Network," in IEEE Access, vol. 8, pp. 73182-73192, 2020

[2] M.Lavanya, V. Natarajan, "LWDSA: lightweight digital signature algorithm for wireless sensor networks", Sādhanā, Indian Academy of Sciences, vol. 42, no. 10, pp. 1629–1643 2017

[3] C. Wang, G. Xu and J. Sun, "An enhanced three-factor user authentication scheme using elliptic curve cryptosystem for wireless sensor networks", Sensors, vol. 17, no. 1, 2017.

[4] R. Amin, S. K. H. Islam, N. Kumar and K. K. R. Choo, "An untraceable and anonymous password authentication protocol for heterogeneous wireless sensor networks", J. Netw. Comput. Appl., vol. 104, pp. 133-144, Feb. 2018.

[5] J.Ryu, H.Lee, H.Kim and D.Won, "Secure and efficient three-factor protocol for wireless sensor networks", Sensor, vol. 18, no. 12, 2018.

[6] J. Jung, J. Moon, D. Lee, and D. Won, "Efficient and security enhanced anonymous authentication with key agreement scheme in wireless sensor networks," Sensors, vol. 17, no. 3, p. 644, 2017.

[7] VS Naresh, S. Reddi, and N.V. Murthy, "Provable secure lightweight multiple shared key agreement based on hyper elliptic curve Diffie–Hellman for wireless sensor networks", Inf. Secur. J., Global Perspective, vol. 29, no. 1, pp. 1–13, 2020.

[8] I. Santos-González, A. Rivero-García, M. Burmester, J. Munilla, and P. Caballero-Gil, "Secure lightweight password authenticated key exchange for heterogeneous wireless sensor networks", Inf. Syst., vol. 88, 2020

[9] S. Athmani, A. Bilami, and D. E. Boubiche, "EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs", Future Gener. Comput. Syst., vol. 92, pp. 789–799, Mar. 2019

[10] J. Lee, S. Yu, M. Kim, Y. Park and A. K. Das, "On the Design of Secure and Efficient Three-Factor Authentication Protocol Using Honey List for Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 107046-107062, 2020

[11] S. Mesmoudi, B. Benadda, A. Mesmoudi, "Skwn: Smart and dynamic key management scheme for wireless sensor networks", International Journal of Communication Systems, vol. 32, no. 7, 2019

[12] M.S. Yousefpoor, H. Barati, "DSKMS: a dynamic smart key management system based on fuzzy logic in wireless sensor networks", Wireless Networks, vol. 26, pp. 2515–2535, 2020

[13] HN Noura, R. Melki, A. Chehab and M. Mansour, "A Physical Encryption Scheme for Low-Power Wireless M2M Devices: a Dynamic Key Approach", Mobile Netw Appl, vol. 24, pp. 447–463, 2019

[14] A. Karrar, T. Almutiri, S. Algrafi, N. Alalwi, and A. Alharbi, "Enhancing Salted Password Hashing Technique Using Swapping Elements in an Array Algorithm", vol. 9, no. 1, pp. 21–25, 2018.

[15] M. M. Bachtiar, T. H. Ditanaya, S. Wasista and R. R. Kurnia Perdana, "Security Enhancement of AES Based Encryption Using Dynamic Salt Algorithm," International Conference on Applied Engineering (ICAE), pp. 1-6, 2018

[16] Sutriman and B. Sugiantoro, "Analysis of Password and Salt Combination Scheme To Improve Hash Algorithm Security" International Journal of Advanced Computer Science and Applications(IJACSA), 10(11), 2019.

[17] J. Jeong, D. Woo and Y. Cha, "Enhancement of Website Password Security by Using Access Log-based Salt," 2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBIoTS), pp. 1-3, 2019

[18] NS. Ali, M.H. Alattar A.A. Farawn, "Anti-continuous collisions user-based unpredictable iterative password salted hash encryption", In Int. J. Internet Technology and Secured Transactions, volume 8, page 619–634, 2018.

[19] EMWR Chowdhury, M.S. Rahman, A.B.M.A.A.Islam, and M.S. Rahman, "Salty secret: Let us secretly salt the secret", In 2017 International Conference on Networking, Systems and Security (NSysS), pp. 115–123, 2017.

[20] H. Tan and I. Chung, "Secure Authentication and Group Key Distribution Scheme for WBANs Based on Smartphone ECG Sensor," in IEEE Access, vol. 7, pp. 151459-151474, 2019

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details