Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: VI Número: Edición Especial Artículo no.:30 Período: Agosto, 2019.

TÍTULO: Formas de mejorar la seguridad de la información en redes de sensores inalámbricos.

AUTOR:

1. Máster. Delshad Wasimi.

RESUMEN: Las redes de sensores inalámbricos (WSN) se han estudiado recientemente para una amplia gama de aplicaciones en la comunidad. Dado que la operación de seguridad de la información en WSNs es responsabilidad de los nodos de la red, la seguridad en esta red es más que en otras redes, debido a limitaciones inherentes de los recursos y la salud computacional de los nodos sensores. La seguridad en las redes de sensores enfrenta diferentes desafíos que la seguridad en las redes de computadoras tradicionales, y la provisión de seguridad de la información en estas redes es cada vez más problemática. Este documento aborda una revisión exhaustiva de cómo mejorar la seguridad de las redes de sensores, especialmente la seguridad de los protocolos de información.

PALABRAS CLAVES: redes de sensores inalámbricos, protocolos, seguridad de la información, WSNs.

TITLE: Ways to improve the information security in Wireless Sensor Networks.

AUTHOR:

1. M. Sc. Delshad Wasimi.

ABSTRACT: Wireless Sensor Networks (WSNs) have recently been studied for a wide range of applications in the community. Since the operation of information security in WSNs is the responsibility of the network nodes themselves, the security of the network in this network is more than other networks, on the one hand due to the inherent limitations of resources and the computational heath of the sensors nodes, security in sensor networks encounter different challenges than security in traditional computer networks, and the provision of information security in these networks is becoming more and more problematic. This paper addresses a comprehensive review of how to enhance the security of sensor networks, especially the security of information protocols.

KEY WORDS: Wireless sensor networks, Protocols, Information security, WSNs.

INTRODUCTION.

Information security in virtual environments and a new area of WSNs has always been emphasized as one of the infrastructures and basic requirements for the development and deployment of wireless networks (Zissis, et al, 2012, Bose, 2013).

Although absolute security is unattainable both in the real environment and in the virtual environment, it is possible to create a level of security that is sufficiently adequate in almost all environmental conditions. In wireless sensor networks, there are many security challenges that must be addressed by cloud wireless networks providers to convince users to use this technology (Zhang, 2013, Adeela, et al, 2013). One of the most important issues is ensuring the user's data is inaccurate and unavailable. For the user, the security process used to store data in the wireless networks is very obscure, long, and vague (Rasheed, 2014).

The application of WSNs is a clear solution for different markets, such as manufacturing and environment monitoring, military and critical infrastructure monitoring, and, more recently, in energy-efficiency and healthcare sectors, due to their great capabilities in acquiring and transmitting

data and processing them for different purposes. Security, network topology, and communication protocol are vital issues in the current application of WSN. Various methods should be used according to the application requirements, such as distance, number of transmissions during a period of time, authentication needs, and rate of the frequency band, to name a few (Tarigonda, 2015). In several references, cited in Reference (Kshetri, 2013, Bravo,2017, Sood, 2012) multiple techniques have been proposed to meet different WSN security threats mitigation. The security situation, which involves an interaction between the defender(s) and attacker(s), can be directly mapped to a game among players in which each player strives to promote its benefit.

In Reference (Tarigonda, 2015), the authors introduce a brief interpretation of the different game techniques presented in the literature to address WSN security. In addition, an overall view of the desired WSN properties in terms of security fulfillment is presented. This work analyzes game theory-based approaches for the mitigation of different WSN security threats according to state-of-the-art literature on the topic, classifying those approaches into two main categories, namely, cooperative games and non-cooperative games, and each summarizes the involved defense strategies based on game theory.

The proposed secure mechanism in Reference (Rong Chunming, 2011) is based on a physical layer security technique, the switch-and-stay combining scheduling scheme. The algorithm requires that the jammer node has the information from a global channel state of both the legitimate channel and the eavesdropper's channel. The achievable secrecy rate has been obtained in closed-form expressions, providing the secrecy outage probability and the effective secrecy throughput, so it is possible to configure the best parameter values for a particular WSN deployment.

Cognitive-Radio WSNs are a promising type of network capable of sensing the radio spectrum in its surroundings and of modifying its behavior to improve the overall performance of the WSN. This approach was achieved in Reference (Sood, 2012), where the authors propose a cooperative secure

transmission strategy. In order to further analyze this dependency, the authors study the transmission rate and the primary WSN secrecy rate for a given sensor node to optimally allocate its transmission power considering different threshold conditions. Valuable information related with the power allocation strategy is described with different scenarios to exhibit the performance tradeoff between the transmission rate and the secrecy outage probability. The main conclusion is that, to guarantee the secure transmission of the primary WSN, the cognitive radio should dynamically adjust its transmission power.

As has been previously discussed, the spreading use of WSNs requires the increase of security measures and protection/mechanisms to reject attacks or information leakage. This situation is more evident when dealing with multiuser communications. In Reference (Abdalzaher et al, 2016), the authors depict a typical scenario where a multiple antenna base station acts as the router for multiple nodes in the WSN. The architecture tries to extend the battery lifetime of WSN nodes while providing good secrecy performance. The correct selection of the jammer node increases the performance on secrecy for the WSN.

DEVELOPMENT.

Overall information security objectives.

The overall security objectives include:

• Accessibility

• Integrity that can include correctness and undeniably

• Trust and confidence

How can we provide secure information in WSNs? Security is sometimes incorrectly integrated into public discussions with other concepts such as privacy, information sharing, intelligence gathering, and research. The privacy of individuals has been coupled with the ability of individuals to control

the other people access. Therefore, a good security can protect the privacy of individuals in a WSNs environment, but the information exchanged in these environments often includes personal information that is considered to be personal information about them.

In addition, research can be viewed as an important component of security by looking at current information in WSNs (Yang, 2016). To this end, we must set the appropriate boundary between the two definitions of WSNs and information security. In most researchers' research, there is no distinction between these two definitions, Von Solms and Niekerk in 2013 (Wang et al, 2016) have identified the distinction between these two definitions, as shown in Figure 1.

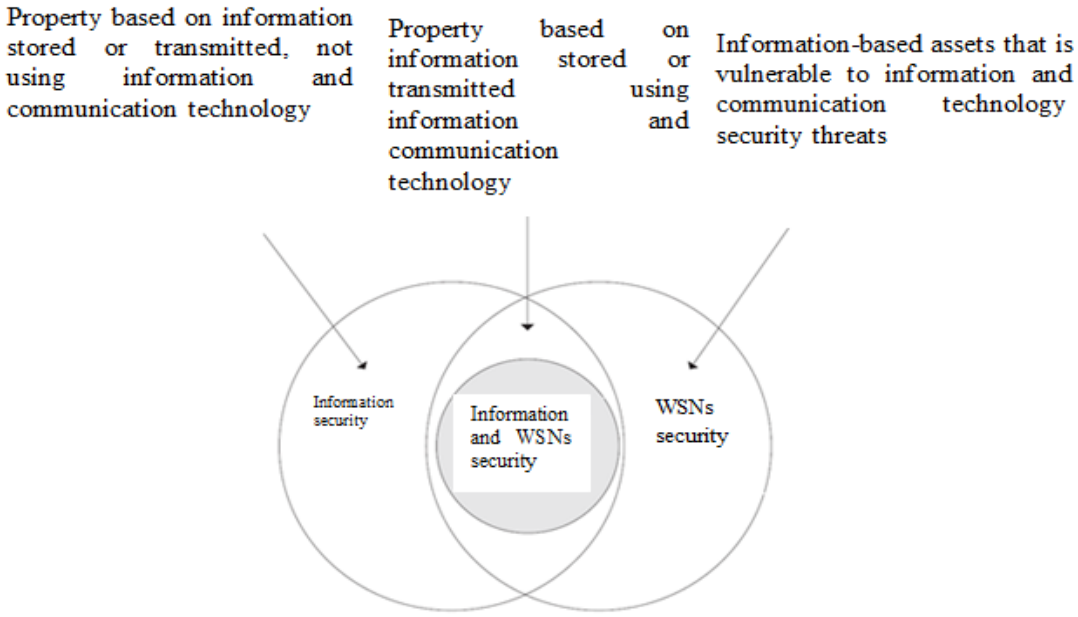

Figure 1: Relationship between information and WSNs security, information security and WSNs security.

In fact, security is often different from information security, although it is often used as an equivalent phrase for information security. Information security is an asset protection against potential damage caused by various threats and vulnerabilities. On the other hand, security does not necessarily just

protect WSNs itself; it also protects the factors that work in WSNs and each of their assets that can be accessed through WSNs (Diaz, 2016).

The most prominent feature of IT is social networking that has been highly welcomed and has become part of the lives of individuals (von et al, 2013). In recent years, there has been an unprecedented increase in the use of online social networks. About 300 online social networking systems register more than half a billion users and collect information. As a result, online social networks store a huge amount of personal information and possibly sensitive users and their interactions. This information is usually personal and they are intended to see specific audiences. However, the popularity of online social networks does not only attract honest users, but also attracts groups with opposing interests (Bargh et al, 2004).

The variety and complexity of the goals and pattern of using online social networks inevitably threatens to violate privacy for all users of online social networks as the exchange of information and Internet sharing. Creating a personal profile and using various online social networking applications, the likelihood of easy sharing of information with selected audiences or the general public and facilitating social interactions among users is one of the main motivations for users to join these networks and disclosing personal information in online social networks is a two-edged sword (Zhang and sun, 2010).

On the one hand, it is inevitable and even compulsory to be exposed if people want to participate in social societies. Visibility of user profiles and public display of communications, like the list of friends is essential for the implementation of the core and main features of online social networks, such as information search and social transmissions. On the other hand, leak of personal information in particular the person's identity may lead to devastating attacks from the real world and virtual worlds such as ambush, slander, personal spam and phishing. One cannot deny that today information of capital is important for any new organization. So, protecting information security is very important

and the first priority of many organizations. Unfortunately, there is no specific rule that we can guarantee a 100% security of information (Gross and Acquisti, 2005).

On the other hand, with the increase in the number of users, the issue of data storage has also played a key role; storage of online data in the WSNs, so access to stored data is possible from distributed resources. However, WSNs environment enjoys many challenges in terms of security, confidentiality and data access control. Secure access control plays an important role in protecting privacy and preventing unauthorized users from accessing WSNs services and data (Krishnamurthy and Wills, 2008).

One method for securing this environment is to use encryption methods to encrypt data during processing, storage and transfer processes. Different designs, among traditional encryption schemes, identity-based encryption and character-based encryption can be used to encrypt data in the WSNs environment (Cyril and Ramesh Kumar, 2014).

Specifically, in contrast to security, intrusion is placed, which is in fact one of a kind of threats, when a computer system connects to a network, is exposed to high risk. One of the threats that exist in a computer system is intrusions. Any unauthorized access to a computer's resources is referred to as a computer penetration. To defend these threats, many security techniques have been studied over the past decades, including cryptography, firewalls, intrusion detection and anomaly (Youssef and Emam, 2011). This research is a review of the research on WSNs methods in order to enhance the security of information and in this section, which is a common point of information security and WSNs security (Figure 1) and prevents crime that is usually based on the influence of this sector.

Review on cryptographic systems.

Security is one of the branches of computer security, which deals specifically with Internet security, based on finding solutions and algorithms against attacks. An unsecure Internet channel is considered

for data exchange, one example of which is phishing. Multiple cryptographic methods are used to protect data transmission (Shyam Nandan, 2015).

Encryption means converting information into an unrecognizable form and transferring it, and then returning the encrypted data to the original and readable state. In general, there are three types of encryption and matching methods: Symmetric-key Cryptography, Public-key Cryptography (Or asymmetric), and hash functions, each of which is described below (Menezes et al, 2017).

***Secret key cryptography*.**

In this type of encryption, both parties intending to exchange information use a common key to encrypt and decrypt the password. Symmetric key algorithms can be divided into two categories:

• Block algorithms

• Current algorithms

Block algorithms encode data from a block of a number of bytes over a period of time, while their current algorithms encode bytes in bytes or even bit-to-bit.

Unfortunately, the symmetric-key algorithms have three problems that limit their use in the real world:

• In order for the computer communication parties to be able to exchange information securely using the symmetric token algorithm, they must first exchange an encryption key. Secure encryption key exchange can be very difficult.

• Because they want to send or receive messages, both parties must have a copy of the keystroke for themselves and keep it safe if the key of one of the parties is corrupted and the other side is not aware of this issue. The second party may send a communication for the first party and then that message can be exploited by using the tampered key.

• If any user wants to use this algorithm to secure communication, each duplex link is to be encrypted. By increasing the number (N2-N) /2 N, a different user will need a unique need, that's for users; this number will quickly be uncontrollable. Some algorithms that are used in the field of computer security are summarized below:

Data Encryption Standard (DES) is a block encryption algorithm that uses a 56-bit password key and has several operating modes, depending on what purpose it is used for.

Blowfish: A fast, compact, and simple encryption block algorithm developed by Bruce Shaker. The algorithm has a variable length key, which can reach up to 448 bits, and optimized for performance on 32-bit and 64-bit processors.

(AES) Rijndael: Rijndeal is an extremely fast and compact encryption algorithm that can handle 128 to 192 or 256-bit password strings.

Disposable pads: The Pad system is disposable. In this type of algorithm, the communication parties share a keystroke consisting of a long string of random bytes. By converting each byte of a message by a byte key, the message is encrypted and decrypted, and then that byte key disappears and is never used again. Because the random key is non-repetitive, even a key search attack will not work, because with each key, any possible message can be generated.

Public Key Cryptography.

These keys are mathematically interrelated but knowing a key does not make it possible for a person to recognize another key. The following list summarizes today's common-sense key-code systems:

RSA: RSA can also be used to encrypt information as well as the basis of a digital signing system. Digital signatures can be used to prove the authenticity or authenticity of digital information. In this system, closed password key is a kind of implementation that can be used in any length.

Diffie-Hellman: it is a system for exchanging cryptographic keys between communication parties. In fact, the method is not an encryption and decryption method, it's a way of developing and exchanging a private key on a public communications channel.

DSA / DSS: The DSS Digital Signature Standard was developed by the US National Security Agency and was selected by the National Institute of Standards and Technology (NIS) as a general FIPS information standard.

The DSA is based on the DSA digital signature algorithm. Although DSA permits a key for any key, the FIPS DSS only allows keys with a length of 512 and 1024 bits.

Message summary functions: message inside a file (large or small) is converted to a large number, usually 128 to 256 bits long. Many summary functions have been provided that are already being used. The most famous of them is the MD5. The message summary functions, due to their features, are also an important part of today's cryptographic systems. Summary of messages is the basis of most digital signing standards. Today's digital signature standards stipulate that the document's summary should be signed instead of the entire document. Message summaries can also be easily applied to pieces of message identity authentication programs that communicate with each other and confirm the message.

Table 1 shows the uses of the public key encryption system and according to this table, the summary method looks like all security tips.

Table 1- Applications of public key encryption system.

Algorithm	Encryption / decryption	digital signature	Key exchange
RSA	yes	yes	yes
Diffie-Hellman	no	no	yes
DSS	no	yes	no
message summary	yes	yes	yes

Hash functions.

Hash algorithms do not use the key as opposed to symmetric and asymmetric algorithms, and the encryption operation is performed unilaterally on the information. The function of these functions is that by applying a hash function on a text, an abstract of that text is obtained. A hash is a process that mathematically reduces the volume of a stream of data with a constant length, and acts like a human finger. And in general, the purpose of the hash function is data integrity. Almost all hash cryptographic functions include duplicate use of a compression function (Lamberger et al, 2009).

In this way, signing a large amount of data can be achieved by verifying the signature of the root node. The Merkel tree program security depends on the security of the hash functions and the original signature creation program, such as RSA, DSA, and ECDSA (Merkle, 1984), and has math problems and decompression problems and discrete logarithms.

The role of symmetric and asymmetric algorithms and hash functions in maintain information security in WSNs.

Symmetric algorithms generally require less computer processing power than asymmetric algorithms and are therefore far faster. However, the problem remains that in symmetric algorithms the key must be exchanged before secure communication, while in the asymmetric algorithm, the shared key used to decrypt the message will never be disclosed, and far more secure than symmetric algorithms, and it's decrypted in symmetric algorithms, such as a common encryption key and decryption key.

In hash functions it is not possible to deduce the input by output and have a high speed and guarantee the integrity of the message. But in general, while information sent using these algorithms is encrypted, invaders can still attack them, but with the lengthening of the keys, the keys can be somewhat prevent intrusion.

Overview of cryptographic methods in WSNs.

Somani et al (2010) have presented a digital signage with the RSA algorithm scheme, to ensure data security in the WSNs and to do this; they used a few lines of crushing algorithm to crunch the data. These lines are called message summaries. Then the software encrypts the message summary with its private key to generate a digital tag. The digital signage is decoded by the software with its private key and the public key of the sender to the message summary.

Vamsee and Sriram (2011) combine polyphyrous and vision techniques as well as SDES standard data encryption simplified data structures and the DES data encryption standard. Where a block of 62-bit size is taken from a simple text that is fixed and this simple 62-bit text is split into two halves using the "black box", which has a half-width of 2 bits, while the left-hand side has 6 bits, then the six bits enter the "superior function" block where these six bits are further separated into two halves, the first two bits representing the rows and the last four bits representing the column. By identifying these rows and columns, the corresponding value can be selected. This function is applied to all 8 outputs of the Debian block, and the result of the black box is again 62 bits. Then, these bits are again divided into 2 new eighths, and similarly the two bits are aligned together to form the right half. Finally, the right and left halves of the XOR get to the left half of this arrangement. This process is repeated three times.

Shuai and Jianchuan (2011) used the RSA algorithm to data and encrypt binary Diffie-Hellman to ensure data security when exchanging keys. In the proposed method, in order to communicate directly and securely between the client and the cloud without any third-party server, a message header is added to the front of each data packet. When a user sends a data storage request to the cloud server, then the cloud server generates the public key, private key, and user ID on the server. The two work is done before sending the cloud to the end user, first adding the message header to the data, and the second encrypting the data, including the message header using the password key and when the user

requests a cloud to the server, then the cloud server checks the received message's header and removes the unique identifier for the server in the cloud's SID information and if SID is found, it will respond to the request of the user, otherwise the request will be canceled.

Sood (2012) has introduced a technique to ensure the availability, integrity and confidentiality of data in the cloud using 128-bit encryption of SSL secure socket layers which can also be upgraded to 256-bit encryption. User who wants to access cloud data, before giving access to the encrypted data, must have a username and passphrase.

the data user to the cloud, and then the cloud service provider makes a key and encrypts the user's data using the RSA algorithm and data stores in its data center. When requests cloud of a user, provider of cloud-based service verifies the user authentication and encrypted data given to the user that can be decrypted by calculating the private key.

Mohammed et al (2012) have provided a three-layer data security model, in which each layer performs different tasks to secure data in the cloud. The first layer is responsible for the correctness, the second layer performs the data encryption task, and the third layer executes the data retrieval function.

Singh et al (2012) implemented the RC5 algorithm to ensure data security in the WSNs. An encrypted data is transmitted even if the data is stolen; there is no corresponding key to decrypt it.

Lan et al (2013) proposed a basic encryption technique for RBE, to secure the data in the WSNs and the basic access control WSNs architecture has the role of RBAC and allows organizations to store data safely in the cloud, while the codified information of the structure of organizations in the WSNs is maintained.

Taeho et al (2013) defined four sovereignty, owner of the data, data consumer, server and N governance feature, in which the attribute property sets of sovereignty were divided into N sets separated by category. The owner of the data takes the public key from each state and encrypts the

data before sending it to the server. When data is requested, sovereigns make a private key and send it to the consumer and the consumer can only download the file if it is verified by the server. Ching-Nung and Jia-Bin (2013) have proposed two types of secure processing, one that requires a trusted third party and the other. These two types of Diffie-Hellman EDDH echo curves and symmetric bi-variable polynomial-based encryption are used to ensure data security in WSNs.

Abolghasemi et al (2013) introduced position-based encoding techniques using user location and geographical location where a geodynamic encryption algorithm was implemented on the WSNs and the user's computer, giving data to the label of the name of the company or the person working in the company. When the data is requested, then the same label is searched and retrieved and the corresponding information is retrieved.

Rewagad and Pawar (2013) have proposed a technique using digital signage and Diffieh Helmman key exchange combined with advanced encryption standard encryption algorithms to protect the confidentiality of data stored in the WSNs. This plan is referred to as a trilogy mechanism because it provides the authenticity, security of data and validation simultaneously.

Lee et al (2013) defined the private key access structure for the user, and encryption with key-determination policy, including four steps for setting up, encryption, key generation and decryption. In the first step, the encryption algorithm receives the input security parameter and then returns the public key and the original key as output. The public key is used by the sender to encrypt the message and the primary key is used by the authorized center to generate the user's private key. The algorithm receives a set of tags, a public key and a message for encryption, and returns the text in the output. In the key generation stage, the access structure, public key and key are used to generate the user's private key.

Decryption can be implemented as a recursive algorithm. If the tags are in the text code, with the structure of access available in the user's private key, the user can reveal the contents of the message. This cryptographic scheme is suitable for providing fine-grained access control, since it specifies which user can access what parts of the data item and what kind of operation can be performed on that type of data.

Manjusha and Ramachandran (2014), have worked on the code- text policy, this scheme is like a key-based design. In a key-based design, access policy, in the private keys of users, but in this scheme, access policies are defined in the code of the text. This cryptographic scheme also includes four steps for launch, encryption, key generation and decryption. In the first step, it starts with an input security parameter and generates the public key and the primary key in the output. The encryption step with message inputs, the public key and the access structure returns the text of the code as output. In the key generation stage, the user receives the private key by receiving the primary key and attributes as input and in the decryption process, by encrypting the text and the private key, the decryption is performed if the set of tags in the user's private key satisfies the text access control structure.

Ostrovsky et al (2007) worked on the cryptographic design with non-uniform access structures. This scheme is the development of a cryptographic scheme with key decision policy with the difference in the structure of access to this project; negative words have been used to describe the tags. In this design, the encryption algorithm includes four steps for launch, encryption, key generation and decryption. Inputs and outputs in these four stages are like the key-encryption scheme, with the difference in the structure of the key-oriented layout's uniform access, in this scheme, the structure becomes non-uniform access. This scheme has a flexible access structure, due to the possibility of using negative words in describing the characteristics, it creates other cryptographic schemes, but its overheads are high due to the use of negative keywords for attributes.

Wang et al (2011) have proposed hierarchy-based encryption; this design is a combination of a hierarchical identity-based cryptographic design and a feature-based encryption scheme with a text-coded policy. In this design, the hierarchy of generating identity-based encryption keys, for generating keys, and a normal quarterly form for describing pre-emptive control policies has been used. In this plan, five factors, including storage service, data owner, root permission center, domain registrar and data users play a role. The storage unit allows storage and data sharing with the user's desks for the data owner. The role of the data owner is encryption and data sharing. The role of the authorized root canals is the production of system parameters, range keys and their distribution. The role of the authorized domain center is to manage the domains in the subcategories and all the users in those domains and deliver the keys to them. The role of the user is to use private keys to reveal a text code.

Compare encryption methods based on security performance.

Shabir et al (2016), have proposed criteria for evaluating cryptographic designs in terms of security performance in WSNs:

1. Data privacy: before data is uploaded in WSNs, the data is encrypted by the owner or the sender, so unauthorized users cannot access the nature of the encrypted information.

2. Finite Access Control: in one group, the system must grant different access rights to users and members of that group. Users are part of a group, but each user can have different access rights. Accordingly, access in one group is not the same for all members.

3. Scalability: when authorized users increased, the system should continue to function effectively. Therefore, the number of authorized users should not affect the performance of the system.

4. User responsibility: if users are not authorized, the user can provide private users with unauthorized users.

5. Unauthorized user: the system should be able to be used when the user leaves the system.

It automatically regains its access rights and then the user will not have access to the data.

6. Resistance to user collusion: users should not be able to reveal cached data by collusion and collaboration.

Now, based on the six criteria for evaluating cryptographic designs, we formulate a table in terms of security performance in WSNs, with rows of security measures and its columns are 16 encryption methods in Section 2 and if the encryption method has that criterion, the score is 1 and if not 0, it will have points.

Table 2: Comparison between criteria and cryptographic methods.

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Data privacy	0	1	1	1	0	1	1	1	1	0	1	0	1	1	1	1
2	Finite Access Control	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1
3	Scalability	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
4	User responsibility	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	1
5	Unauthorized user	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
6	Resistance to user collusion	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	total	2	3	4	3	2	3	3	3	3	3	3	2	4	5	4	6

According to the results of Table 2, according to Shabir et al [49], in the evaluation of cryptographic schemes in terms of security performance in WSNs, the best way of encryption is Wang et al [38] Hierarchy-based encryption.

CONCLUSIONS.

In this study, after defining cryptographic methods, we have investigated different methods of encryption in WSNs by various researchers in order to improve the security of information and communication technology in WSNs, and then with the help of the criteria proposed by Shabir et al (2016), we have evaluated these methods and obtained the best cryptographic methods. However, many researchers have devoted their efforts to minimizing the issue of data security in this domain with a variety of solutions, as explained in this study.

The results of the review of this study point to the fact that most researchers are interested in encryption techniques to enhance data security in the WSNs.

BIBLIOGRAPHIC REFERENCE.

1. Zissis, Dimitrios, and Dimitrios Lekkas (2012) Addressing cloud computing security issues. Future Generation Computer Systems 28.3: 583-592.
2. Bose, Ranjit, Xin Luo, and Yuan Liu. (2013) The Roles of Security and Trust: Comparing Cloud Computing and Banking. Procedia-Social and Behavioral Sciences 73: 30-34.
3. Zhang, Xuyun, et al. (2013) An efficient quasi-identifier index-based approach for privacy preservation over incremental data sets on cloud. Journal of Computer and System Sciences.
4. Waqar, Adeela, et al. (2013) A framework for preservation of cloud users' data privacy using dynamic reconstruction of metadata. Journal of Network and Computer Applications 36.1: 235-248.
5. Rasheed, Hassan. (2014) Data and infrastructure security auditing in cloud computing environments. International Journal of Information Management 34.3: 364-368.

6. Tarigonda, Siva, A. Ganesh, and Srinivasulu Asadi (2015) Providing Data Security in Cloud Computing using Novel and Mixed Agent based Approach. International Journal of Computer Applications 112.6.
7. Kshetri, Nir (2013) Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy 37.4: 372-386.
8. Bravo, I., Palomar, E., Gardel, A., & Lázaro, J. L. (2017). Trusted and Secure Wireless Sensor Network Designs and Deployments. Sensors (Basel, Switzerland), 17(8), 1787. doi:10.3390/s17081787
9. Sood, Sandeep K. (2012) A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications 35.6: 1831-1838.
10. Tarigonda, Siva, A. Ganesh, and Srinivasulu Asadi (2015) Providing Data Security in Cloud Computing using Novel and Mixed Agent based Approach. International Journal of Computer Applications.
11. Rong Chunming, Nguyen Son T. (2011) Cloud trends and security challenges. In: Proceedings of the 3rd international workshop on security and computer networks (IWSCN 2011).
12. Sood, Sandeep K. (2012) A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications 35.6: 1831-1838.
13. Abdalzaher M.S., Seddik K., Elsabrouty M., Muta O., Furukawa H., Abdel-Rahman A. (2016) Game Theory Meets Wireless Sensor Networks Security Requirements and Threats Mitigation: A Survey. Sensors. 16:1003. doi: 10.3390/s16071003.
14. Yang M., Zhang B., Huang Y., Yang N., Guo D., Gao B. (2016) Secure Multiuser Communications in Wireless Sensor Networks with TAS and Cooperative Jamming. Sensors. 16:1908. doi: 10.3390/s16111908.

15. Wang D., Ren P., Du Q., Sun L., Wang Y. (2016) Reciprocally Benefited Secure Transmission for Spectrum Sensing-Based Cognitive Radio Sensor Networks. Sensors. 16:1998. doi: 10.3390/s16121998.
16. Diaz A., Sanchez P. (2016) Simulation of Attacks for Security in Wireless Sensor Network. Sensors. 16:1932. doi: 10.3390/s16111932
17. Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97-102. http://dx.doi.org/10.1016/j.cose.2013.04.004
18. Bargh, J. A., & McKenna, K. Y. A. (2004). The Internet and social life. Annual Review of Psychology, 55, 573–590.
19. C. Zhang, M. J Sun, (2010) Privacy and Security for Online Social Networks: Challenges and Opportunities. IEEE Communications Society, vol 24, pp. 13–18.
20. R. Gross and A. Acquisti (2005) Information Revelation and Privacy in Online Social Networks, Proc. WPES '05, Alexandria, VA.
21. B. Krishnamurthy and C. E. Wills (2008) Characterizing Privacy in Online Social Networks, Proc. WOSN '08, Seattle, WA.
22. Bethencourt J., Sahai A., Waters B. (2007) Ciphertext policy attribute-based encryption; in Proceedings of IEEE Symposium on Security and Privacy, pp. 321-334.
23. Cyril B. R., Ramesh Kumar S. B. (2015) Cloud Computing Data Security Issues, Challenges, Architecture and Methods A Survey, International Research Journal of Engineering and Technology, Vol. 2, PP. 848-857, 2015.
24. Ahmed Youssef and Ahmed Emam (2011) Network intrusion detection using data mining and network behaviour analysis.
25. Shyam Nandan Kuma R. (2015) Review on Network Security and Cryptography.

26. Menezes, A. J.; van Oorschot, P. C.; Vanstone, S. A. (2007) Handbook of Applied Cryptography, ISBN 0-8493-8523-7

27. M. Lamberger, F. Mendel, C. Rechberger, V. Rijmen, M. Schlaer (2009) Rebound distinguishers: results on the full Whirlpool compression function; Advances in Cryptology, Proceedings Asiacrypt'09, LNCS 5912, M. Matsui, Ed., Springer, Heidelberg, pp. 126-143

28. Merkle R. (1989) Certified digital signature, Proc Advances in Cryptology (Crypto' 89), Berlin: Springer-Verlag, 218-238.

29. Somani, U., Lakhani, K., & Mundra, M. (2010, 28-30 Oct. 2010). Implementing digital signature with RSA ncryption algorithm to enhance the Data Security of cloud in Cloud Computing. Paper presented at the Parallel Distributed and GridComputing (PDGC), 2010 1st International Conference on.

30. Vamsee K. and Sriram R. (2011) Data Security in Cloud Computing; in Journal of Computer and Mathematical Sciences Vol. 2, pp.1-169.

31. Shuai, H., & Jianchuan, X. (2011, 15-17 Sept.2011). Ensuring data storage security through a novel third-party auditor scheme in cloud computing. Paper presented at the Cloud Computing and Intelligence Systems (CCIS), 2011 IEEE International Conference on.

32. Sood, S. K. (2012). A combined approach to ensure data security in cloud computing. Journal of Network and Computer Applications, 35(6), 1831-1838.

33. Mohamed, E. M., Abdelkader, H. S., & El-Etriby, S. (2012,14-16 May 2012). Enhanced data security model for cloud computing. Paper presented at the Informatics and Systems (INFOS), 2012 8th International Conference on.

34. Singh, J., Kumar, B., & Khatri, A. (2012, 6-8 Dec. 2012). Improving stored data security in Cloud using Rc5 algorithm. Paper presented at the Engineering (NUiCONE), 2012 Nirma University International Conference on.

35. Lan, Z., Varadharajan, V., & Hitchens, M. (2013). Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage. Information Forensics and Security, IEEE Transactions on, 8(12), 1947-1960.
36. Taeho, J., Xiang-Yang, L., Zhiguo, W., & Meng, W. (2013). Privacy preserving cloud data access with multi-authorities. Paper presented at the INFOCOM, 2013 Proceedings IEEE.
37. Ching-Nung, Y., & Jia-Bin, L. (2013). Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing. Paper presented at the Biometrics and Security Technologies (ISBAST), 2013 International Symposium on.
38. Abolghasemi, M. S., Sefidab, M. M., & Atani, R. E. (2013). Using location-based encryption to improve the security of data access in cloud computing. Paper presented at the Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on.
39. Rewagad, P., & Pawar, Y. (2013) Use of digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. Paper presented at the Communication Systems and Network Technologies CSNT), 2013 International Conference on.
40. Lee C., Chung P., Hwang M., (2013). A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments, International Journal of Network Security, Vol.15, No.4, PP.231-240
41. Manjusha R., Ramachandran R., (2014). Comparative Study of Attribute Based Encryption Techniques in Cloud Computing", International Conference on Embedded Systems, pp. 116-120
42. Ostrovsky R., Sahai A., and Waters B., (2007). Attribute-based encryption with non-monotonic access structures,", in Proceedings of the 14th ACM conference on Computer and communications security, pp. 195-203.

43. Wang G., Liu Q., Wu J., and Guo M., (2011). Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," Computer & Security, vol. 30, pp. 320-331.

44. Shabir M. Y., Iqbal A., Mahmoo Z., Ghafoor R., (2016). Analysis of Classical Encryption Techniques in Cloud Computing", Tsinghua Science and Technology, Vol. 3, pp. 102-113

DATA OF THE AUTHORS.

1. Delshad Wasimi. Graduated Msc, Department of Computer Engineering, Mehrastan University, Astaneh-ye Ashrafiyeh, Gilan Province, Iran. Email: d.wasimi@aftermail.ir

RECIBIDO: 4 de julio del 2019. **APROBADO:** 19 de julio del 2019.