ISSN 2394-739X

IJRSET

International Journal for Research in Science Engineering and Technology

A REVIEW ON WIRELESS SENSOR NETWORKS FOR CRYPTOSYSTEM AND HASH BASED MULTIFACTOR AUTHENTICATION

[1] C. Venkatachalam, [2] Dr. A. Suresh
[1] Ph.D Research Scholar (PT), [2] Head, Dept. of Computer Science
[1]Periyar University, Salem-11, [2] Sona College of Arts and Science, Salem-5.

ABSTRACT- Wireless sensor network security pulls in considerations of numerous specialists around the globe. Security is utilized with attributes of authentication, uprightness, protection, nonrepudiation and privacy. The security benefits in WSN need to ensure the data imparted over network and assets from the assaults. Security and authentication during information communication are testing one in WSN. For secure communication in WSN, cryptographic and steganographic techniques are utilized. The information are sent or gotten to by any hub in network after authentication measure to keep from unapproved clients to get to the data. Our exploration work is concentrated for protected information communication with assistance of authentication techniques.

Keywords: [Wireless Sensor Networks;Cryptosystem; Hash Based Multifactor Authentication;Integrity.]

1. INTRODUCTION

Wireless sensor networks (WSNs) are a grounded unavoidable innovation that speaks to an ideal detecting segment in the Internet of things. They are made out of minimal effort and low force gadgets, called sensor hubs, which sense the climate, measure the gathered data and trade data through a wireless association and air quality observing. A wireless sensor network is an organization to screen physical or natural conditions, for example, temperature, sound, pressure, and so on the improvement of wireless sensor networks was inspired via air contamination observing, water quality checking, land side recognition, woods fire location, territory observing, etc. In spite of the fact that there are numerous applications in wireless sensor network space, human medical services applications play the significant job. In human medical care, sensors are utilized to screen the patient's wellbeing status, for example, temperature level, sugar level, heart beat rate, circulatory strain. Wireless sensor networks, as arising network innovations, have risen steadily as of late. They can acquire a ton of definite and solid data in the organization appropriated region whenever and anyplace; consequently, they are generally utilized in military safeguard, industry, horticulture, development and metropolitan administration, biomedical and ecological observing, calamity help, public wellbeing and antiterrorism, perilous and hurtful local controller, etc which are greatly accounted by numerous legislatures. Wireless sensor networks have a significant logical and reasonable worth.

1.1 Wireless Sensor Network

Wireless Sensor Networks (WSNs) can be characterized as a self-designed and foundation fewer wireless networks to screen physical or ecological conditions, for example, temperature, sound, vibration, pressing factor, movement or poisons and to helpfully go their information through the organization to a fundamental area or sink where the information can be noticed and dissected. A sink or base station acts like an interface among clients and the organization. One can recover required data from the organization by infusing questions and assembling results from the sink. Commonly, a wireless sensor network contains countless sensor nodes. The sensor hubs can convey among themselves utilizing radio signs.

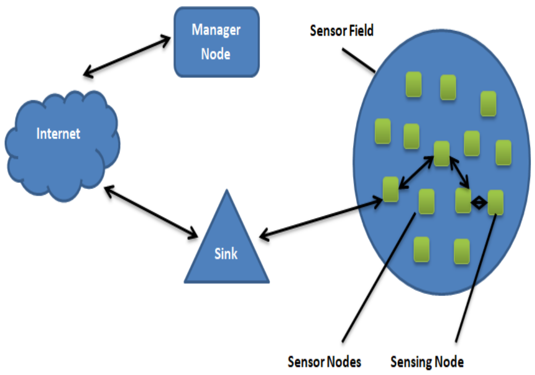

Figure 1.Wireless Sensor Network

A wireless sensor node is outfitted with detecting and registering gadgets, radio handsets and force segments. The individual nodes in a wireless sensor network (WSN) are innately asset compelled: they have restricted preparing speed, stockpiling limit, and correspondence transfer speed. After the sensor nodes are conveyed, they are answerable for self-putting together a proper network framework regularly with multi-bounce correspondence with them. At that point the locally available sensors begin gathering data of interest. Wireless sensor gadgets likewise react to questions sent from a "control site" to perform explicit directions or give detecting tests. The working method of the sensor nodes might be either persistent or occasion driven. Global Positioning System (GPS) and neighbourhood positioning algorithms can be utilized to acquire area and positioning data. Wireless sensor gadgets can be outfitted with actuators to "act" upon specific conditions. Wireless Sensor Network comprises of spatially appropriated independent sensors to screen ecological states of the earth. The advancement of wireless sensor networks was persuaded by military applications, for example, war zone reconnaissance. Wireless Sensor Networks (WSN) are conveyed at basic spots like reconnaissance, checking, air terminals, combat zone applications consequently making sure about wireless sensor networks is a difficult assignment.

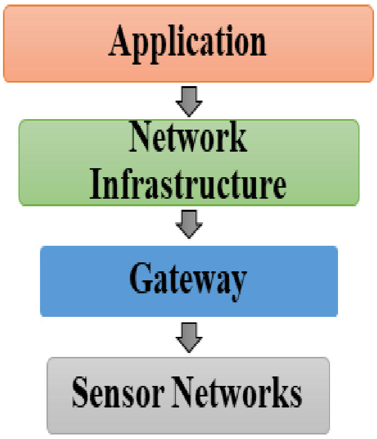

Figure 2.Secured Wireless Sensor Network

Following are the Security Requirements in Wireless Sensor Networks.

1.1.1 Confidentiality

Confidentiality prerequisite is needed to guarantee that delicate data is very much secured and not uncovered to unapproved outsiders. The confidentiality target assists with securing data going between the sensor hubs of the network or between the sensors and the base station from divulgence, since a foe having the fitting gear may snoop on the correspondence. By snooping, the enemy could catch basic data, for example, detecting information and steering data. In light of the affectability of the information taken, a foe may cause serious harm since he can utilize the detecting information for some unlawful purposes for example damage, shakedown. For instance, contenders may utilize the information to create a superior item for example security checking sensor application. Besides, by taking steering data the foe could bring his own pernicious hubs into the network trying to catch the whole correspondence.

1.1.2 Authentication

As in conventional frameworks, authentication techniques confirm the personality of the members in a communication, recognizing in this way genuine clients from gatecrashers. On account of sensor networks, it is fundamental for every sensor hub and base station to be able to confirm that the information got was truly send by a confided in sender and not by an enemy that fooled authentic hubs into tolerating bogus information. On the off chance that such a case occurs and bogus information are provided into the network, at that point the conduct of the network couldn't be anticipated and the greater part of the occasions won't result true to form. Authentication objective is fundamental to be accomplished when bunching of hubs is performed. Bunching includes gathering hubs dependent on some quality, for example, their area, detecting information and so on and that each group generally has a group head that is the hub that gets its group together with the remainder of the sensor network (implying that the communication among various groups is performed through the group heads).

1.1.3 Integrity

Proceeding onward to the integrity objective, there is the peril that data could be changed when traded over shaky networks. Absence of integrity could bring about numerous issues since the results of utilizing incorrect data could be heartbreaking, for instance for the medical services area where lives are jeopardized. Integrity controls should be executed to guarantee that data won't be changed in any startling manner. Numerous sensor applications, for example, contamination and medical services observing depend on the integrity of the data to work with exact results; it is unsuitable to gauge the extent of the contamination brought about by synthetic compounds waste and discover later on that the data gave was inappropriately adjusted by the industrial facility that was found close by the checked lake. Subsequently, there is dire need to ensure that data is heading out from one finish to the next without being blocked and altered all the while.

1.1.4 Freshness

One of the numerous assaults dispatched against sensor networks is the message replay assault where a foe may catch messages traded among hubs and replay them later to create turmoil to the network. Information freshness objective guarantees that messages are crisp, implying that they comply with in a message requesting and have not been reused. To accomplish freshness, network conventions should be planned in an approach to distinguish copy parcels and dispose of them forestalling likely mistake.

1.1.5 Secure Management

Management is needed in each framework that is comprised from multi-segments and handles delicate data. On account of sensor networks, we need secure management on base station level; since sensor hubs correspondence winds up at the base station, issues like key conveyance to sensor hubs to build up encryption and directing data need secure management. Besides, bunching requires secure management also, since each gathering of hubs may incorporate an enormous number of hubs that should be confirmed with one another and trade information in a secure way. What's more, bunching in every sensor organization can change powerfully and quickly. In this way, secure conventions for bunch management are needed for adding and eliminating individuals and confirming information from gatherings of hubs.

1.1.6 Availability

Availability guarantees that administrations and data can be gotten to at the time that they are required. In sensor networks, there are numerous dangers that could bring about loss of availability, for example, sensor hub catching and refusal of administration assaults. Absence of availability may influence the activity of numerous basic constant applications like those in the medical care area that require an all day, every day activity that could even bring about the death toll. In this manner, it is basic to guarantee strength to assaults focusing on the availability of the framework and discover approaches to fill in the hole made by the catching or disablement of a particular hub by allotting its obligations to some different hubs in the organization.

1.1.7 Quality of Service

Quality of Service objective is a major migraine to security. Also, when we are talking about sensor networks with all the constraints they have, quality of service turns out to be significantly more obliged. Security components should be lightweight with the goal that the overhead caused for instance by encryption should be limited and not influence the presentation of the organization. Execution and quality in sensor networks include the opportune conveyance of information to forestall for instance engendering of contamination and the exactness with which the information detailed match what is really happening in their current circumstance.

1.2 Wireless Sensor Network Applications

1. Military applications: Wireless sensor networks are likely an essential piece of military order, control, correspondences, registering, insight, front line observation, surveillance and focusing on systems.

2. Area monitoring: In area monitoring, the sensor nodes are sent over a district where some wonder is to be checked. At the point when the sensors identify the occasion being observed (heat, pressure and so on), the occasion is accounted for to one of the base stations, which at that point makes a proper move.

3. Transportation: Real-time traffic data is being gathered by WSNs to later take care of transportation models and ready drivers of blockage and traffic issues.

4. Health applications: Some of the health applications for sensor networks are supporting interfaces for the impaired, coordinated patient monitoring, diagnostics, and medication organization in clinics, tele-monitoring of human physiological information, and following and monitoring specialists or patients inside a clinic.

5. Environmental sensing: The term Environmental Sensor Networks has created to cover numerous applications of WSNs to geology research. This incorporates sensing volcanoes, seas, glacial masses, woods and so forth.

6. Structural monitoring: Wireless sensors can be used to screen the development inside structures and foundation, for example, spans, flyovers, banks, and burrows and so on empowering Engineering practices to screen resources distantly without the requirement for exorbitant site visits.

7. Industrial monitoring: Wireless sensor networks have been created for hardware condition-based upkeep (CBM) as they offer critical expense reserve funds and empower new functionalities. In wired systems, the establishment of enough sensors is frequently restricted by the expense of wiring.

8. Agricultural area: Utilizing a wireless network liberates the rancher from the upkeep of wiring in a troublesome climate. Water system robotization empowers more effective water use and lessens squander.

2. PROPOSED FRAMEWORK

In the accompanying, we clarify Investigation on Combinatorial Asymmetric Key Cryptosystem and Hash Based Multifactor Authentication Techniques for Secured Data Communication in Wireless Sensor Network how to convey the necessary keys and key chains on sensor hubs earlier organization. This cycle is refined in key arrangement stage; at that point in shared key revelation stage, we express how two sensor hubs can find a typical key for their safe communications for Wireless Sensor Networks.

2.1 Cryptography

Cryptography is the technique of composing privileged insights. This makes sure about data and data from any inside or outer assaults. Subsequently, it gives respectability, privacy, non-renouncement and validness to the mystery data. The idea of cryptography depends on two fundamental terms-plain text and cipher text. The first message is known as the plain text and the encoded adaptation of the message is known as the cipher text. The cipher is at long last unscrambled to get the first message. Cryptography is extensively grouped into two primary sorts. These are symmetric key encryption technique and asymmetric key encryption technique.

2.1.1 Symmetric Key Cryptography

Symmetric key cryptography is likewise called mystery key or shared key cryptography. In this kind of system, the sender and recipient share a typical key for both encryption and decryption. The strategy follows self-accreditation technique for example the key is self-guaranteed. The key should be shared through mystery correspondence. In the event that it is undermined, at that point the encoded message can be effortlessly decoded by the assailant. This kind of cryptographic strategy is required on the grounds that it provides quicker assistance without utilizing numerous assets. Different calculations have been grown so far to describe symmetric key cryptography. These are AES, DES, 3DES, Blowfish.

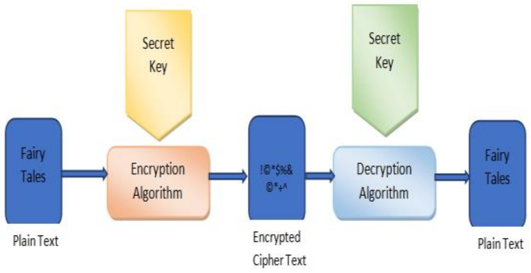

Figure3: Symmetric Key Cryptography

2.1.2 Asymmetric Key Cryptography

The asymmetric key cryptography is known as public key cryptography. In this technique, the sender uses a public key of the receiver for encryption and the receiver uses his private key to decrypt the message. The concept of self-certification is absent here instead digital signatures are used to certify the keys. This method is more convenient and provides better authentication as the privacy remains intact. There are various algorithms to implement this encryption mechanism. These are RSA, Diffie-Hellman, ECC and Digital Signature Algorithm.

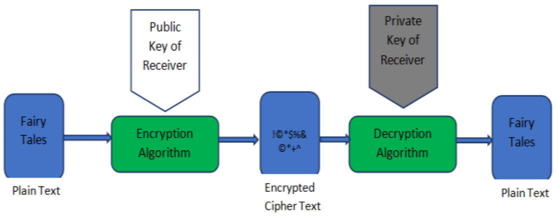

Figure4. Asymmetric Key Cryptography

2.3 Hash Based Multifactor Authentication

Multi-Factor Authentication (MFA) is an authentication method that requires the authenticating party (be it a person, software or a hardware module) to produce several separate identifiers (or "factors") that are indicative to its identity, instead of the previously standard single identifier, usually a password, required by default in many systems. High dependency on digital services, whether business or personal, has changed the way companies and regulators see user authentication. As the threat of cyber-attack targeting authentication mechanisms specifically keep growing (most attacks on business data today leverage stolen or weak passwords to some degree [Verizon DBIR]), and countless incidents of account takeovers and data breaches are reported annually, all parties realize that standard password-dependent authentication is a huge security liability and require users and clients to use some sort of MFA.

2.3.1 Multifactor Authentication Techniques

Multifactor Authentication Techniques is the client ID and secret phrase authentication system are the most old-style strategy among authentication techniques on the web; notwithstanding, it is a weak technique against snooping or replay assaults. The multifactor authentication calculation makes a one-of-a-kind single direction computerized unique mark that speaks to the substance of IoT bundles. To adapt to the three previously mentioned situations, which are miniature IoT worldview authentication, full scale IoT worldview authentication, and miniature large scale worldview authentication.

These are planned dependent on the accompanying suspicions:

1. Each sensor gadget has three secure keys—two privates (K1 and K2) and one public (K_DSA: key for direct access control)— which are put away during gadget programming.
2. Each sensor gadget static or portable knows about its area.
3. Sink is a confided in base station.
4. A sensor gadget can't utilize TOTP on the grounds that it has restricted assets which influence the accuracy figuring of the supreme time that is needed in a coordinated TOTP.
5. Each IoT gadget has two secure keys—one private (KI, ID) and one public K_DSA.
6. An IoT gadget and the sink have a capacity to actualize TOTP and the TEOTP.
7. A sink or a base station has an information base that stores the total subtleties, everything being equal, and IoT gadgets.

2.3.2 Multi-factor authentication methods

MFA recognizable proof can be classified into three kinds:

Knowledge factors (something the client knows) – Common models are email addresses, username-secret key blends, answers to security questions, and the CVV on the rear of a Visa.

Possession factors (something the client possesses) – Examples of this verification type incorporate a cell phone, USB token and a card peruser.

Inherence factors (something the client is/has) – This confirmation type relates to remarkable actual credits that are characteristic to a solitary individual, for example, unique mark perusers, retinal sweeps and voice acknowledgment.

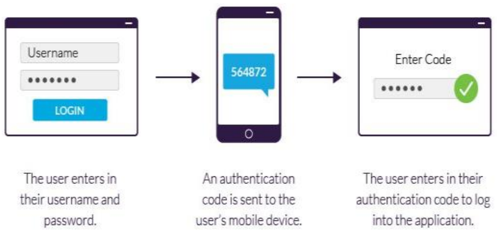
Username
•••••••
LOGIN
564872
Enter Code
••••••
The user enters in their username and password.
An authentication code is sent to the user's mobile device.
The user enters in their authentication code to log into the application.

Figure 3.Multi-factor authentication

2.4 Wireless Sensor Networks for Hash Based Multi Factor Authentication

Wireless sensor network, WSN is an ad-hoc like network that work self-sufficiently. It is actualized in different applications including checking and detecting exercises drives by the flexibility of the technology. It utilizes efficient sensor node that housed various detecting units to screen actual changes of the climate, for example, temperature, light force, level of radiation, pressing factor and then some. It is additionally generally used to screen tremendous topographical zone requiring little to no effort on the grounds that the economical hardware and simplicity of organization. Sensor nodes regularly have restricted memory and preparing abilities, and furthermore should endeavour to monitor power. Security conventions/calculations are normally the inverse, requiring memory for key stockpiling, preparing overhead for encryption/authentication, and don't actually consider power scant applications. To make sure about the message transmission safety efforts, for example, encryption, decryption and authentication are executed into the framework. Encryption and decryption guarantee classification and cover the message from untouchables.

Authentication permits entities to approve the integrity of the message and furthermore confirm the authority of the communicating devices. Also, it can frustrate replay assault and it use hash function as a mean of security. Other than hash function, Message Authentication Code, MAC, Digital Signature and Encryption function are different choices that are usually used to make authenticator for authentication measure. Regardless of all the invaluable, WSN activity experiences asset's restriction. Wireless sensor is a gadget that has restricted capacity, battery life and computational ability. Sadly, because of the idea of wireless correspondence in WSNs, enemies can undoubtedly snoop the traffic, mimic different clients, infuse fake information or change the substance of real messages during the multi-jump sending. Subsequently, authentication components should be actualized to shield messages from different noxious assaults. Here, authentication includes both source and message authentication. While source authentication guarantees a recipient that the got information begins from the asserted source, message authentication ensures that the information from the source is new and unaltered.

CONCLUSION

In this paper the emphasis was made on exploiting multiple security technologies and partnered highlights to plan a multifaceted authentication and key administration strategy. Basically,canteredon using cryptosystem-based client authentication, in the proposed work, multiple security highlights are utilized to infer a novel security framework. Likewise, in contrast to traditional security frameworks, in this paper the spotlight was made on achieving security for WSN, yet in addition on maintaining minimum execution compromise because of added security model over local WSN-routing convention. Reproduction based execution evaluation has uncovered that our proposed multifactor authentication. The proposed model showed satisfactory execution for WSN based frameworks.

REFERENCE

[1]. K. HimaBindu, Ch. LavanyaAishani, M.Kamalakar, "A Secure Key Exchange Scheme in Wireless Sensor Networks Using Diffie Hellman," International Journal of Innovative Research in Computer and Communication Engineering, vol. 4, no 9, pp. 16338-16343, Sept 2016.

[2]. D. Djenouri And L. Khelladi, A. NadjibBadache, "A Survey Of Security Issues In Mobile Ad Hoc And Sensor Networks," IEEE Communications Surveys & Tutorials, vol. 7, no. 4, pp.2-28, Fourth Quarter 2005.

[3]. Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials 2006; 8: 2–23.

[4]. M. L. Das, "Two-factor user authentication in wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1086–1090, 2009.

[5]. L.-P. Zhang and Y. Wang, "An ID-based authenticated key agreement protocol for wireless sensor networks," Journal of Communications, vol. 5, no. 8, pp. 620–626, 2010.

[6]. MohitSaxena, "Security In Wireless Sensor Networks - A Layer Based Classification," Cerias Tech Report 2007-04.

[7]. Hirsch, Frederick J. "SSL/TLS Strong Encryption: An Introduction". Apache HTTP Server. Retrieved 17 April 2013. The first two sections contain a very good introduction to public-key cryptography.

[8]. Ferguson, Niels; Schneier, Bruce (2003). Practical Cryptography. Wiley. ISBN 0-471-22357-3.

[9]. Katz, Jon; Lindell, Y. (2007). Introduction to Modern Cryptography. CRC Press. ISBN 978-1-58488-551-1.

[10]. Kavitha T, Sridharan D. Hybrid design of scalable key distribution for wireless sensor networks. International Journal of Engineering and Technology 2010; 2 (2): 136–141.

[11]. Chong C, Kumar S. Sensor networks: evolution, opportunities, and challenges. Proceedings of the IEEE 2003; 91(8): 1247–1256.

[12]. Arun Kejariwal, " Cryptic primes", IEEE Potentials, pp. 43-45, Feb./Mar. 2004, IEEE.

[13]. Minoru Kuribayashi and Hatsukazu Tanaka, "Fingerprinting Protocol for Images Based on Additive Homomorphic Property", IEEE Transactions on Image Processing, vol. 14, no. 12, pp. 2129-2139, Dec. 2005, IEEE.

[14]. SubramaniaSudharsanan, " Shared Key Encryption of JPEG Color Images", IEEE Transactions on Consumer Electronics, vol. 51, no. 4, pp. 1204-1211, Nov. 2005, IEEE.

[15]. G. Boato, N. Conci, and V. Conotter, F.G.B. De Natale, and C. Fontanari, "Multimedia asymmetric watermarking and encryption", Electronics Letters, vol. 44 no. 9, April 2008, IEEE.