International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 2 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT195214

Critical Security Mechanism Designed for Data Transmission in Wireless Sensor Networks using Hierarchical Cloud Server

P. Lokesh Kumar Reddy[1], Dr. K. Ramesh Reddy[2]

[1]Research Scholar, Department of Computer Science, Rayalaseema University, Kurnool, Andhra Pradesh, India

[2]Assistant Professor, Department of Computer Science, Vikrama Simhapuri University, Nellore, Andhra Pradesh, India

ABSTRACT

The rapid advancement of pervasive computing, IoT and wearable systems, given rise to low-power internet-based systems in elimination of distance complications by application of Wireless Sensor Networks, which consists of sensor, server and Cloud servers to sense various environmental readings and monitor the condition based on the data. Due to the association of vital data, and transferring it over an insecure and public communication channel, there is a critical prerequisite for sensor authentication, data integrity and data privacy. In this context many researchers had proposed various schemes for user authentication and secure data transmission over Cloud server. In this paper we proposed a three-factor user authentication and key agreement protocol for cloud server and claimed that the proposed protocol is efficient, secure and lightweight. The experimental analysis shows that the proposed scheme is resistance to well-known cryptographic attacks. Though the proposed scheme resists major cryptographic attacks, after in-depth analysis, we demonstrate that the scheme overcome many security pitfalls such as failure to resist replay attack, known session-specific temporary information attack, and failure to resist stolen-verifier attack.

Keywords : Wireless Sensor Network, Cloud Server, Security, Sensors

I. INTRODUCTION

In recent years, many technologies such as Internet of Things, Edge Computing etc., are being developed to provide more convenience to the human beings in the world. The data is also emerging largely from various sensor devices and to store such huge amount of data in a local server is very difficult. A cloud computing came into existence to store such enormous amount of streaming data and it became more prominent technology. Even though cloud computing technology is ruling the world, it has some limitations such as Latency, security etc. To overcome that drawbacks edge computing came into picture. In edge computing, the data processes in the edge of a network without going to process the data in a centralized server and it respond instantaneously. For all the technologies which were briefly described above needs data, that data is being generated by the wireless sensor network devices. These devices are using in everywhere to collect the data, storing and transferring the data to the correspondent servers. In wireless sensor networks, storage nodes will gather data from nearby sensors and answer queries from the sink of the network. The storage nodes serve as an intermediate tier between the sensors and the sink for storing data and processing queries. Storage nodes bring three main benefits to sensor networks. First, sensors save power by sending all collected data to their closest storage node instead of sending them to the sink through long routes. Second, sensors can be memory-limited because data are mainly stored on

storage nodes. Third, query processing becomes more efficient because the sink only communicates with storage nodes for queries. The inclusion of storage nodes also brings significant security challenges. As storage nodes store data received from sensors and serve as an important role for answering queries, they are more vulnerable to be compromised, especially in a hostile environment. A compromised storage node imposes significant threats to a sensor network. First, the attacker may obtain sensitive data that has been, or will be, stored in the storage node. Second, the compromised storage node may return forged data for a query. Third, this storage node may not include all data items that satisfy the query. So, number of attacks can be made by the attackers to access the gathered information. Due to the high cost, number of attacks will be increased on sensor networks such as false data injection attack, clone attack, black attack and selective forwarding attack. A novel technique has to be developed to prevent attackers from gaining information from both sensor collected data and sink issued queries, which typically can be modeled as range queries, and allows the sink to detect compromised storage nodes when they misbehave. For privacy, compromising a storage node should not allow the attacker to obtain the sensitive information that has been, and will be, stored in the node, as well as the queries that the storage node has received, and will receive. Note that we treat the queries from the sink as confidential because such queries may leak critical information about query issuers' interests, which need to be protected especially in military applications. For integrity, the sink needs to detect whether a query result from a storage node includes forged data items or does not include all the data that satisfy the query. There are two key challenges in solving the privacy and integrity-preserving range query problem. First, a storage node needs to correctly process encoded queries over encoded data without knowing their actual values. Second, a sink needs to verify that the result of a query contains all the data items that satisfy the query and does not contain any forged data. The main problem in wireless sensor networks is reliability because of its rapid growth, the attacker's tries to access the information while transmitting the data from sensor to sink or from the stored data in sensor or storage node. The wireless sensor network follows wait-backtrack and resurrecting method. Where the error occurs while transmitting the data from sensor to sink, the transmitters stops and wait to transmit the data. If any data is lost then it backtracks to the sensors there again it corrects the data and starts transmitting the data to sink node. To resolve this problem, the reliability check has to be done at each layer in different ways. If any, apply backtracking instead of using another sink node to process the data because the cost of hardware is extremely high, to get the reliable data but, this takes more time. Now-a-days smart sensors are using in various applications such as in health care, agriculture etc to increase memory functions, data processing ability, independent power sources, communication functions, etc. The smart sensor devices are arranged in different areas to collect the information easily they are using independent power sources so, the fluctuations won't be happen. The sensors can be arranged in different areas such as either on earth, space or in air. The communication between the sensors can be done by using MAC-layer. This layer will reduce the energy consumption and also it maintains some threshold level to transmit the data error free and with low latency.

II. RELATED WORK

Internet of Everything (IoE) is increasing prominently because every communication between people, things, data and process is done through the network. So, the risk is more for the data which we had collected because the attackers can attack easily. The collected data can be sent from the sensor to the sink without any loss of information requires more energy consumption to the sink node. If the reliable

data is not reached to the sink node due to the attacks held on transmission path then energy consumption is very low. The energy consumption is proportionally relating to the number of packets reached to the sink node. The transmitting path must be trustable; it should not provide a scope to the attackers to access the information. The already used path cannot be advisable to send the data or information to the sink node because the attackers can easily identify the path. So, every time while transmitting the data, a new path has to be used to transmit the data to the sink node. To overcome all the limitations, a data authentication has to be used to secure the data. Jiawei Tang, Anfeng Liu, Ming Zhao, and Tian Wang suggested a novel technique to secure data collection in wireless sensor networks called an Aggregate Signature based Trust Routing (ASTR) scheme. In this scheme initially the data which has been collected from different sensors nodes are to be aggregated with each other into one sensor transmission. So this scheme uses trust routing scheme to reach the data very effectively and safely. If the sink node does not get data packets but it gets abstracts then it will notify the sender to send the data packets again. By this the sender came to know that the data is attacked by the attackers so, he won't send the data in the same path as he sends previously. In this paper the trust routing algorithm works effectively in reaching the data packets to the sink and also the comparisons can be done on the performance of the schemes. Finally the results of comparison in this paper shows that aggregate Signature based Trust Routing (ASTR) scheme will reach the data safely to the sink node and also reduces the redundant data.

To guarantee the safe transmission of data by preventing the attacks such as elective forwarding attacks or black hole attacks form attackers, a Karlof and Wagner proposes multipath routing technique. In this method, it uses k paths to send the data to the sink node. If these k paths are compromised then the error attacks so it needs some probabilistic protection. So, the data packets can be divided into n shares and these are sent by k paths to the sender. If any of the path is attacked then the sink node can automatically restores the lost data packet with the k shares. If the data packets reached to the sink are less than the k data packets then the entire transmission will be lost. This method also gives effective results while transmitting the data to the sink node without any data loss.

While transmitting the data from the sender to the receiver i.e., to the sink node, the attackers may attack the transmission path to access the data. If the data is lost while transmitting, the recipient has to send response to the sender to retransmit the data packets again. This retransmission is common in today's environment. The retransmission can occurred due to the following cases such as data packets delay, attacks, altered etc. To retransmit the data to the receiver takes more delay, increases the energy consumption and decreases the throughput while focusing on the reliable data transfer. When the reliable data is not reached to the sink node then the sink node sends an acknowledgement to send the data packets again. There is also another method called redundancy method, which stores the copies of data packets into it. It uses forward correction i.e. in this method the sender can't check for the lost data packet, it directly send the whole data packets to the sink node. Compared to the retransmission the redundancy works well. To improve the reliability, Run Ye, Azzedine Boukerche, Houjun Wang, Xiaojia Zhou and Bin Yan propose a technique called RESIDENT: A Reliable reSIDuE Number System for reliable data transmission from the sensor to the sink node, which uses hybrid automatic repeat mechanism in every hop for effective and reliable data. In this an algorithm is also introduced to improve the performance, through put and decreasing the energy consumption, latency time. The Redundant residue Number System mainly focuses on the data

transmission by improving the reliability of data packets with the help of some redundancies. To check the reliability of a data, in this paper they consider transmission delay, energy capacity, processing capacity, algorithm complexity and power consumption. By taking all these aspect into consideration they check the reliability of a data. In further enhancement, the researcher can concentrate on predicting the bit error rate and also adapting the length of redundant information.

Internet of things is using in wide area of applications like logistics systems etc. In these systems a smart sensor is used to collect the data from its own or from other sensor nodes and this data can be transmitted to sink node reliably. For the reliable data transmission, in this paper the authors Kyunghee Sun and Intae Ryoo proposed a technique called Sensor Node Group Management MAC to group the smart sensor nodes by using the sink group-ID and which can help the data to be transmitted directly towards the sink. Initially the sink node has to create a group-id and these id has to be sent to the nearby smart sensor nodes. For this, the sink node uses advertisement packet which contain the group-id and its version of setting the group-id. The sink node sends its packet to all nearby sensor nodes to accept its packet. If a node does not contain a group id then it accepts the request and adds id in it. If the received sensor node is already having group-id even though it receives new request then it resets to the new one because it came far away to the older version of group-id. After grouping the sensor nodes the data has to be transmitted to the sink node by using the smart sensor nodes of upper-level. To reach data to the sink node, it has to transmit the collected to the upper level of sensor node on the same group to control the through put, energy consumption etc., and to reach the reliable data to the sink node.

This method also support the mobility of sensor node, if the data is moved away from one group to another then the group id has to be resetted. The mobility of sensor node causes mainly for the following two reasons: 1. when the distance between the sink node and the smart sensor node is relatively high. 2. If the sensor node is not able to communicate with the upper level of sensor node i.e., if the upper-level sensor node sends a request to send (RTS) to the sensor node for three times even though the smart sensor nodes doesn't give clear to send (CTS) to the upper level of sensor node.

The proposed method also sets buffer threshold limit for each and every sensor node and it size is depends on the group. The node which is nearer to the sink node has more size when compared to the far node. In every smart sensor node, it collected the data of its own and also from its lower level sensor nodes in the buffer. If the data in the sensor nodes are comparatively higher than the size of buffer then the data can be sent to the adjacent sensor node or to the next level of sensor nodes. The size of buffer will be decided by using the following formulae: $B\ i = bw \times B\ t$.

In this paper, the authors concentrate on the delay of data transmission. Sometimes the delay can be accepted but if someone needs the data very urgently but delay happen in those cases, the authors proposes a technique called urgent data transmission. The data which is urgently required is given higher priority when compared with the ordinary data. To differentiate the urgency data with the ordinary the data to data a flag called 'Fu' is used. If the data contains fu is 1 then that data is said to be an urgent data and it has given higher priority to transmit the sink node else Fu is 0. This technique concentrates on number of issues and finally it has proven to be energy efficient by comparing the performance of this technique in all aspects with others. In future, the researchers can also improve the performance by increasing the travel distance of nodes, buffer

thresholds or by enhancing the techniques used for urgent data transmissions etc.

III. OUR CONTRIBUTION

The contribution of the paper is twofold. Firstly, it consists of a brief discussion on Hierarchical Cloud Server based on authentication mechanism for Sensor Network. Secondly, we show that Proposed [3] scheme is susceptible to following attacks. (1) Stolen-verifier attack leading to framing of session key and login request message by an attacker. (2) Replay attack (3) Known session-specific temporary information attack leading to Cloud server bye pass attack, and fails to preserve sensor identity.

1.1. PROPOSED SCHEME

In this section, we describe the various phases of Proposed[3] mechanism, that are (i) registration phase of Cloud server, (ii) registration phase for user, (iii) login phase, (iv) authentication and session key agreement phase. The notations used ate provided in Table 1.

Table 1 : Notations and their meanings

Symbol	Description
Pi	i^{th} user/sensor
MRS	Cloud registration server
MSj	j^{th} Cloud server ($1 \le j \le m$)
PSk	k^{th} physician server ($1 \le k \le p$)
PPIDi	Identity of Pi
PPWi	Password of Pi
MSIDj	MSj Identity
PBi	Pi is the personal biometric information
KMRS	Privacy key for MRS
PSIDk	PSk Identity
KMSj	Privacy key for MSj
KPMjk	Shared secret key in between PSk and MSj
RPi	Pi based Random nonce
KPMjk	Shared secret key in between PSk and MSj
RMSj	MSj based Random nonce
RPSk	PSk based Random nonce
TMSj	Recent time-stamp produced by MSj
TPSk	Recent time-stamp produced by PSk
Δt	utmost transmission delay,
TPi	Recent time-stamp produced by Pi
H (·)	Bio-hashing function [27, 35]
h(·)	Collision-less single-way hash function
Rep(·)	Fuzzy based reproduction algorithm
Gen(·)	Fuzzy based generation algorithm
τi	Biometric parameter of Pi
σi	Biometric key of Pi
$P \oplus Q$	Bitwise XOR of data P with data Q
εt	Error tolerance threshold
$P \| \| Q$	Data P concatenates with data Q

The proposed scheme consists of six phases: (i) pre deployment phase, (ii) registration phase, (iii) login phase, (iv) key agreement and authentication phase, (v) password modification phase (vi) dynamic node addition phase.

1.1.1. Cloud Server Registration Phase:

Let us assume that 'ms' denotes the count of Cloud servers MSj, ($1 \le j \le ms$) that are to be installed initially within the network. We further assume that ms* additional number of Cloud servers MSj, ($ms + 1 \le j \le ms + ms^*$) may be further added in the network, where $ms^* << ms$. For instance, initially ms = 200 Cloud servers that may be installed and in a while we may include ms* = 20 additional Cloud servers after initial employment in the network, based on the demand and the need of health care services depending on the additional users accessibility ratio.

In this context, a Cloud server MSj, (1 ≤ j ≤ ms), was initiated to enable the Cloud services to the remotely located sensors, where they need to go for a unique identity MSIDj as well as send it to the MRS. MRS calculate the secret key Xj = h (MSIDj||KMRS) after analysing MSIDj, where KMRS is devised as 1024-bit secret key for the MRS in the context of security reasons, and revert it back to MSj through a secure channel. Thus, every MSj keeps (MSIDj, Xj). For ms* additional Cloud servers MSp, (ms + 1 ≤ p ≤ ms + ms*), the MRS itself select a distinctive identity MSIDj in addition it also calculate the privacy key Xq = h(MSIDj||KMRS). The computed (MSIDj, Xq) are set aside to the MRS further it will be used afterwards during the user registration phase along with dynamic Cloud server enumeration phase.

1.1.2. User Registration Phase

Initially within this phase, a legal sensor Pi have to register with the MRS to access the health care services from the selected physician server PSk under a Cloud server MSj within the network.

a. Steps in the User registration phase are enumerated as follows :

Step R1: Pi initially inputs his/her preferred identity PPIDi, password PPWi, as well as trace the personal biometrics PBi at the sensor of a specific device. Further Pi produces a 1024-bit random number K, which is maintained confidentially to Pi only. Pi subsequently apply the fuzzy extractor based generation function Gen (·) on the input PBi consecutively to generate the biometric based data key σi along with the public parameter τi as Gen (Bi) = (σi, τi). Note that σi id maintained confidentially with respect to Pi only.

Step R2: Pi computes the pseudo-random password PRPWi as PRPWi = h (PPIDi||K||PPWi) and sends the registration request {PPIDi, PRPWi} to the MRS via a privacy channel.

Step R3: After accepting the enrollment ask for from Pi, the MRS keeps on processing RMj = h (PIDi||Xj) ⊕PRPWi and RMSj = h(MSIDj ||Xj) ⊕PRPWi, for 1 ≤j ≤ ms + ms*. At that point the MRS stores the information{{MSIDj , RMj , RMSj|1 ≤ j ≤ m + ms*},h(•), Gen(•), Rep(•), t} in a brilliant card, say SCPi and sends it to the sensor/client Pi by means of a safe channel, where 'at' is the error resistance limit utilized as a part of fluffy extractor.

Step R4: After accepting the savvy card SCi from the MRS, the client Pi registers ei = h (PPIDi||σi) ⊕ K and fi = h (PPIDi||PRPWi||σi). Pi at that point stores ei and fi in the smart card SCPi. At long last, take note of that the brilliant card SCPi contains the data {MSIDj, RMj, RMSj|1 ≤ j ≤m + m*}, ei, fi, h (•), Gen (•), Rep (•), τi, and 'εt'.

1.1.3. Login stage:

In this stage, a lawful client Pi can get to any restorative server MSj for the medicinal administrations from a doctor server PSk under that therapeutic server MSj at whenever from anywhere through his/her issued savvy card PSCi. This stage contains the following advances:

Step L1: Pi first installs his/her astute card PSCi into a smart card per user of a specific terminal, and after that inputs his/her character PPIDi, watchword PPWi, and moreover imprints the singular biometrics PBi at the sensor

Step L2: SCi then compute sσi* = Rep (Bi, τi),K∗ = h(PPIDi||σi*) ⊕ ei,PRPWi* = h(PPIDi||K∗||PPWi),fi* = h(PPIDi||PRPWi∗ ||σi*).SCi additionally checks the confirmation condition fi*= fi.If it holds, it guarantees that the client Pi passes successfully both secret word and biometric check. Something else, this phase is ended instantly.

Step L3: SCPi further continues to create a random nonce RPi and the present time-stamp TPi. Then SCPi computesM1 = RMj ⊕PRPWi*= h(PPIDi||Xj) ⊕PRPWi ⊕PRPWi*= h(PPIDi||Xj),M2 = RMSj⊕PRPWi*= h(MSIDj ||Xj),M3 = PPIDi⊕ M2,M4 = PPIDi⊕ M1 ⊕RPi,M5 = h(M1||M3||M4||RPi||TPi).SCPi sends the login ask for message {MSIDj, PYIDk, M3,M4, M5, TPi} to the restorative server MSj by means of a public channel, where PYIDk is the character of the doctor server PSk from where Pi needs to get to the medicinal administration.

1.1.4. Session key Agreement and Authentication Phase:

In this stage, a lawful client Pi verifies an accessed physician server PSk and PSk likewise confirms Pi for mutual confirmation reason before they can set up uneven basic session key SKPPS between them for their future secure correspondence. This stage includes the following steps:

Step A1: {MSIDj, PYIDk, M3, M4, M5, TPi} from Pi,MSj confirms the legitimacy of the got time-stamp TPiin the message. Let the login ask for be received by MSj at time TPi*. MSj at that point checks the condition|TPi*– TPi|≤ ΔT, whereΔT means the maximum transmission delay. On the off chance that this condition comes up short, the login asks for message is rejected and furthermore the session is terminated quickly. Something else, MSj executes the next step.

Step A2: MSj keeps on registering M6 = h(MSIDj||Xj) utilizing its own character MSIDj and the mystery key , where Xj = h(MSIDj ||Xc) and Xc is the mystery key of the MRS. MSj then computesM7 = M3 ⊕ M6= PPIDi,M8 = h(M7||Xj)= h(PPIDi||Xj),M9 = M4 ⊕ M7 ⊕ M8= RPi,M10 = h(M8||M3||M4||M9||TPi)= h(h(PPIDi||Xj)||M3||M4||RPi||TPi).MSj additionally checks the condition M10 = M5. In the event that it holds, MSj trusts the validness of the client Pi. Otherwise, MSj ends the session instantly.

On the off chance that the condition M10 =M5 holds, MSj stores the combine (M7, M9) = (PIDi, RPi) in its database. Afterward, when MSj gets the following login request message, say MSIDj, PSIDk, M3*, M4*, M5*, TPi, MSj first checks the legitimacy of the time-stamp TPi. Ifit is legitimate, MSj registers M6* = h (MSIDj ||Xj), M7* =M3*⊕ M6*, M8* = h (M7*||Xj), M9* = M4*⊕ M7*⊕ M8*.After that MSj contrasts M9* and the put away M9 = RPi corresponding to the client Pi's character M7 = PIDi in its database. On the off chance that there is a match, MSj guarantees that the received login ask for message {MSIDj, PSIDk, M3*, M4*, M5*, TPi} is a replay message and disposes of this message .Otherwise, MSj replaces M9 with M9* in its database and treats this message as a crisp message.

Step A3: MSj creates an irregular nonce RMSj and the current time-stamp TMSj. MSj figures M11 =h(MSIDj||PSIDk||KPMjk), where 'KPMjk' is the mystery key shared between MSj and PSk. MSj promote computesM12 = PPIDi ⊕ M11,M13 = h(PPIDi||KPMjk) ⊕RMSj,M14 = PPIDi ⊕ M9 ⊕RMSj = PPIDi⊕RPi ⊕RMSj, M15 = h(PIDi||M11||M12||M13||M14||M9||RMSj||TMSj) MSj at that point sends the confirmation ask for message{MSIDj, PSIDk, M12, M13, M14, M15, TMSj}to the physician server PSk by means of an open channel.

Step A4: After getting the message in Step A3, PSk checks the legitimacy of the got time-stamp TMSj in the message by the condition |TMSj* – TMSj|≤ΔT, where TMSj*is the time when the message is gotten by PSk. On the off chance that it is legitimate, PSk additionally proceeds to computeM16 = h(MSIDj||PSIDk||KPMjk),M17 = M12 ⊕ M16= PPIDi,M18 = M13 ⊕ h(M17||KPMjk)= RMSj,M19 = M14 ⊕ M17 ⊕ M18 = RPi, M20 =

h(M17||M16||M12||M13||M14||M19||M18||TMSj) = h(PIDi||h(MSIDj||PSIDk||KPMjk)||M12||M13||M14||RPi||RMSj ||TMSj).PSk at that point checks the condition M20 = M15. On the off chance that it doesn't hold, the session is ended by PSk. Something else, PSk believes the legitimacy of both MSj and in addition Pi.

Step A5: PSk produces an arbitrary nonce RPSk and the current time-stamp TPSk. PSk likewise computesM21 = h(M17||KPMjk)= h(PPIDi||KPMjk),M22 = M17 ⊕ M19 ⊕RPSk= PPIDi⊕RPi⊕RPSk,M23 = M21 ⊕RPSk= h(PPIDi||KPMjk) ⊕RPSk,SKPPS = h(M17||PSIDk||M19||RPSk||M21||TPSk)= h(PPIDi||PSIDk||RPi ||RPSk||h(PPIDi||KPMjk)||TPSk),M24 = h(SKPPS||M22||M23||M19||RPSk||TPSk).PSk at long last sends the validation answer message {PSIDk,M22, M23, M24,TSk} to the client Pi by means of an open channel.

Step A6: After getting the message in Step A5, the smart card SCi of the client Pi checks the legitimacy of the time-stamp TPSk in the got message by the condition $|TPSk^* - TPSk| \leq T$, where TPSk*is the time when the message is gotten by Pi. In the event that it holds, Pi computesM25 = M22 ⊕ (PPIDi⊕RPi) = RPSk, M26 = M23 ⊕ M25= h (PPIDi||Xk), SKPPS* = h (PPIDi||PSIDk||RPi ||M25||M26||TPSk), M27 = h (SKPPS*||M22||M23||RPi ||M25||TPSk).SCPi at that point checks if M27 = M24. On the off chance that it matches, Pi authenticate PSk, and both Pi and PSk regard SKPPS*=SKPPS as the session key shared between them.

IV. CRYPTANALYSIS OF PROPOSED SCHEME

In this section, we show that Proposed authentication scheme is vulnerable to various major cryptographic attacks, which are detailed in the following subsections.

In this section, we crypt analyze Proposed scheme [3] and demonstrate that their scheme is vulnerable to security attacks. According to the threat model discussed above and depicted in [1, 2, 15, 20, 21], an attacker 'E' can intercept, eavesdrop and alter any message transmitted in the public communication channel. As discussed in [1, 2, 15, 18], the attacker by carrying out power consumption analysis, can extract all the parameters stored in the smart card [1, 2, 11]. Built on these two well accepted assumptions, the proposed scheme is susceptible to subsequent cryptographic attacks.

a. Failure to resist Replay attaack

Sensor (Pj)	Cloud Server (MSj)
Step 1) Login Message 1 :{ MSIDj, PYIDk, M31, M41, M51, TPi1}, using RPi1 as random number.	Step 1) Stores (PIDi, RPi1) in its database.
Step 2) Attacker intercepts the first login message.	
Step 3) Login Message 2: {MSIDj, PYIDk, M32, M42, M52, TPi2}, using RPi2 as random number.	Step 3) In step A2, MSj compares M9'i.e.RPi2 with M9 i.e.RPi1. As both are different, MSj replaces RPi1 with RPi2. i.e.(PIDi, RPi1) -> (PIDi, RPi2) in its database.
Step 4) Now the Attacker replays the intercepted first login message in step 1 above within the valid time frame.	Step 4) MSj compares RPi1 with the current entry i.e.RPi2. As both are different, MSj accepts the replayed message as original.

In Proposed plot they are opposing the replay and MiM assaults in light of match between the irregular number put away in the information base (last effective login message) and the arbitrary number utilized as a part of the current login ask. In this way, the foe can mimic as Pi by replaying any of the blocked login messages from the sensor which are encircled in light of the arbitrary number other than the one as of now put away in the database as appeared in the table above. Henceforth, we can presume that A.K Das et al., plot experiences replay assault, client pantomime assault. Known session-specific temporary information attack.

The compromise or leakage of short-term secret (session specific random values) information should not compromise the generated session key [20, 21, 22, 23, 29]. However, in Proposed scheme, if session specific random numbers i.e.RPi, RMSj and RPSk are compromised, then the adversary can compute the session key SKPPS as follows:

E can intercept and record the transmitted messages {PSIDk, M22, M23, M24, TSk} and {MSIDj, PYIDk, M3, M4, M5, TPi}. With these messages in hand the adversary can frame the session key as follows: Compute:
M23 = M21⊕RPSk => M21 = M23⊕RPSk = h(PPIDi||KPMjk).
M22 = PPIDi ⊕RPi⊕RPSk =>M22 ⊕RPi⊕RPSk = PPIDi With these values, the adversary can compute the session key SKPPS = h (PPIDi||PSIDk ||RPi ||RPSk || h (PPIDi||KPMjk) ||TPSk). Therefore, proposed scheme is vulnerable to Known session-specific temporary information attack in which the compromise of RPi, RPSk, RMSj results in framing of session key by an attacker.

A. Failure to resist stolen-verifier attack

The stolen-verifier attack occurs when an adversary steals the verification table from the server and uses it directly to masquerade as a legal user.'E' as an insider can access to MSj database to get all the pairs of (PPIDi, RPi). As the sensor identity is stored in plain format without any encryption, the adversary can find out all the identities of the sensors. Hence, Proposed fail to preserve the sensor identity PIDi which is a critical requirement in SENSOR NETWORK systems. As the communication messages are transmitted over insecure public communication channel, 'E' can intercept all these communication messages exchanged among the communication entities i.e. {MSIDj, PYIDk, M3, M4, M5, TPi}. M3 = PPIDi ⊕ M2 = >M2 = M3⊕PPIDi. M1 = M4⊕PPIDi⊕RPi the MSj transfers the message {MSIDj, PSIDk, M12, M13, M14, M15, TMSj} M11 = M12 ⊕PPIDi, // from M12. M14 = PPIDi ⊕ M9 ⊕RMSj = PPIDi ⊕RPi ⊕RMSj RMSj = M14⊕PPIDi ⊕RPi // from M14. M13 = h (PPIDi||KPMjk) ⊕RMSj h (PPIDi||KPMjk) = M13 ⊕RMSj // from M13. Now the adversary can frame the session key and the login request by MSj i.e. {MSIDj, PSIDk, M12, M13, M14, M15, TMSj}.

Therefore, proposed scheme is susceptible to stolen verifier attack, once the database or verifier table is stolen by the attacker, the attacker can frame the session key SKPPS and the login request message sent by the MSj to PSk. Hence, we can confirm that Proposed scheme is susceptible to resist Replay attaack, Known session-specific temporary information attack df Now the adversary can frame the session key and the login request by MSj i.e. {MSIDj, PSIDk, M12, M13, M14, M15, TMSj}.

Based on the above discussion, we can confirm that, A.K. das et al scheme is susceptible to stolen verifier attack. Once the database or verifier table is stolen by the attacker, the attacker can frame the session key SKPPS and the login request message sent by the MSj to PSk. Hence, we can confirm that Proposed scheme fails to resist Replay attaack, resist stolen-verifier attack, Known session-specific temporary

information attack, Cloud server bye pass attack, and fails to preserve sensor identity.

User (Pi)	Cloud Server MSj	Physician Server PSk
Inserts SC into a terminal Inputs PPIDi, PPWi Step a) Compute: σi^* = Rep (Bi, τi), K^* = h (PPIDi|| σi^*) ⊕ ei, $PRPWi^*$ = h (PPIDi||K^*||PPWi), fi* = h (PPIDi|| $PRPWi^*$||σi^*). SCi further checks the verification condition fi^* = fi. Step b) Generate : RPi Current time-stamp TPi. Computes: M1 = RMj ⊕$PRPWi^*$ = h(PPIDi||Xj) ⊕ PRPWi ⊕ $PRPWi^*$ = h(PPIDi||Xj) M2 = RMSj ⊕ $PRPWi^*$ = h(MSIDj ||Xj) M3 = PPIDi ⊕ M2 M4 = PPIDi ⊕ M1 ⊕ RPi M5 = h(M1|| M3 || M4|| RPi ||TPi). SCPi sends the login request message {MSIDj, PYIDk, M3, M4, M5, TPi} to MSj →	**Receive:** m1 = {MSIDj, PYIDk, M3, M4, M5, TPi} @ TPi^* Checks if | TPi^*- TPi| < ΔT MSj continues: Compute M6 = h (MSIDj||Xj). M7 = M3 ⊕ M6 = PPIDi M8 = h(M7||Xj) = h(PPIDi||Xj) M9 = M4 ⊕ M7 ⊕ M8 = RPi M10 = h (M8||M3||M4||M9|| TPi) = h (h (PPIDi|| Xj) || M3||M4|| RPi ||TPi). MSj further checks the condition M10 = M5. Generates a random nonce RMSj, TMSj. MSj computes M11 = h (MSIDj || PSIDk || KPMjk). M12 = PPIDi ⊕ M11, M13 = h(PPIDi|| KPMjk) ⊕ RMSj, M14 = PPIDi⊕M9⊕ RMSj = PIDi ⊕ RPi ⊕ RMSj, M15 = h (PPIDi||M11||M12||M13|M14||M9|| RMSj || TMSj). sends the authentication request message {MSIDj, PSIDk, M12, M13, M14, M15, TMSj } →	Step a) PSk checks || TMSj * − TMSj | ≤ ΔT, where $TMSj^*$ is the time when the message is received by PSk. Compute M16 = h(MSIDj ||IDk|| KPMjk), M17 = M12 ⊕ M16 = PPIDi, M18 = M13 ⊕ h(M17|| KPMjk) = RMSj, M19 = M14 ⊕ M17 ⊕ M18 = RPi, M20 = h (M17||M16|M12||M13|| M14 || M19|| M18||TSms) = h (PIDi ||h (MSIDj|| PSIDk || Xk) || M12||M13||M14 || RPi || RMSj || TMSj.). PSk then checks the condition M20 = M15. Step b) PSk generates: RPSk, TPSk. M21 = h(M17||KPMjk) = h(PPIDi|| KPMjk), M22 = M17 ⊕ M19 ⊕RPSk = PPIDi ⊕ RPi ⊕RPSk, M23 = M21 ⊕RPSk = h(PPIDi||KPMjk) ⊕RPSk SKPPS = h(M17||PSIDk||M19|| RPSk ||M21|| TPSk) = h(PPIDi||PSIDk|| RPi || RPSk||h(PIDi|| KPMjk) || TPSk), M24 =h (SKPPS||M22||M23||M19||RPSk || TPSk). PSk sends the authentication reply message {PSIDk, M22, M23, M24, TPSk} to the user Pi via a public channel.
Receive at $TPSk^*$: ← Check : | $TPSk^*$ − TPSk | ≤ T , If it holds, Computes M25 = M22 ⊕ (PPIDi ⊕ RPi) = RPSk M26 = M23 ⊕ M25 = h(PPIDi|| KPMjk)), $SKPPS^*$ = h (PPIDi|| PSIDk|| RPi ||M25||M26|| TPSk), M27 = h($SKPPS^*$||M22||M23|| RPi ||M25||TPSk). SCi then checks if M27 = M24. If it matches, Pi authenticates PSk, and both Pi and PSk treat $SKPPS^*$= SKPPS as the session key shared between them.	{ PSIDk, M22, M23, M24, TPSk }	

Figure 1. Login and authentication phases of proposed scheme

V. ANALYSIS OF WEAKNESS OF PROPOSED SCJHEME

5.1 Analysis on enormous data storage along with computational requirements to generate user smart cards

In Proposed scheme the smart card memory is stored with key-plus-Id combination (Aj, Pj) {1 ≤ j ≤ m + m*.}of all the Cloud servers MSj. Based on the A.K.Das et al. discussion, for a total ofm = 100 and m* = 10, on each user 110 values are stored. If the system contains n users, then a total of (n * 110) hash operations need to be performed to load the smart

card memory of corresponding user which requires huge computation cost from the MS. The major issue is that the user may not interested or in need of data from all the Cloud servers (because a cardiac sensor access only the cardiac and related Cloud servers). Hence storing all the m+m*Cloud server details is a major drawback in proposed scheme. If any Cloud server or sensor server structure has been changed, then all the smart card users' data corresponding to that specific server has to be changed, which is a computationally intensive task.

5.2 Fails to achieve mutual authentication among all the communicating entities.

In Proposed scheme on receiving the login request from the Cloud server MSj, the sensor server responds directly to the sensor by passing the Cloud server. Hence, the mutual authentication among the communicating entities is not achieved.

VI.CONCLUSION

In this paper, initially we proposed a novel scheme for Wireless Sensor Network. Such that the proposed scheme is efficient in resisting most of the cryptographic attacks. Unfortunately, on in-depth analysis, we have verified that their scheme is insecure against several major well known attacks. Thus, their proposed scheme is not suitable for practical application in Sensor Network .In future work; we will come up with an improved version of authentication scheme for Sensor Network which can resist all major cryptographic attacks.

VII. REFERENCES

[1]. Z.Y.Wu, Y.C.Lee, F.Lai, H.C. Lee, and Y.Chung, 'A secure authentication scheme for telecare medicine information systems', springer Journal of Cloud Systems, vol 36, pp:1529–1535, 2012.

[2]. C.Guo, and C.C.Chang, Chaotic maps-based passwordauthenticated key agreement using smart cards.Elsevier journal of Communications in Nonlinear Science and Numerical Simulation,vol 18, pp:1433–1440, 2013.

[3]. R.Amin, and G.P.Biswas, A Novel User Authentication and Key Agreement Protocol for Accessing Cloud Server Usablein SENSOR NETWORK. J. Med. Syst. vol 39,. pp : 1–17, 2015.

[4]. R.Amin and G.P.Biswas,A Secure Three-Factor User Authentication and Key Agreement Protocol for SENSOR NETWORK With User Anonymity,J Med Syst, Aug 2015.

[5]. A.K.Das, V.Odelu and A.Goswami, A Secure and Robust User Authenticated Key Agreement Scheme for Hierarchical Cloud Server Environment in SENSOR NETWORK,J Med Syst, vol 39, 2015.

[6]. J.Srinivas, D.Mishra and S.Mukhopadhyay, 'A Mutual Authentication Framework for Wireless Cloud Sensor Networks',J Med Syst, pp:41:80, 2017.

[7]. S.Challaa,A.K.Das,V.Odelu, N.Kumar,S.Kumari,M.K.Khane and A.V.Vasilakos, 'An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks',Elsevier journal of Computers and Electrical Engineering, pp:1–21,2017.

[8]. D.He, J. Chen, and R. Zhang, 'A more secure authentication scheme fortelecare medicine information systems', springer journal of Cloud systems, vol 36, pp: 1989–1995, 2012.

[9]. T.F.Lee, An Efficient Chaotic Maps-Based Authentication and Key Agreement Scheme Using Smartcards for Telecare Medicine Information Systems,springer journal of Med Syst, vol 37, 2013.

[10]. Jiang, Q., Ma, J., Lu, X., Tian, Y., Robust chaotic map-basedauthentication and key agreement scheme with strong anonymityfor telecare medicine information systems. J. Med. Syst. 2014.

[11]. D.Mishra,J.Srinivas and S.Mukhopadhyay,A Secure and Efficient Chaotic Map-Based Authenticated Key Agreement Scheme for Telecare Medicine Information Systems,Journal of Cloud Systems, vol 38, Oct 2014.

[12]. R.Amin,SK HafizulIslam,G.P.Biswas,M.K.Khan and N.Kumar,A robust and anonymous sensor monitoring system using wireless Cloud sensor networks,Vol 80, Pages 483-495, March 2018.

[13]. A.K.Awasthi, and K. Srivastava, 'A biometric authentication scheme for telecare medicine information systems with nonce', springer jurnal of Cloud systems, vol 37, Oct 2013.

[14]. N.Ravanbakhsh and M.Nazari,An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems,Multimedia Tools and Applications,vol 77, pp 55–88,Jan 2018.

[15]. Hongtao Li,Feng Guo,Wenyin Zhang,Jie Wang and Jinsheng Xing, (a,k)- Anonymous Scheme for Privacy-Preserving Data Collection in IoT-based Healthcare Services Systems,Journal of Cloud Systems,vol 42, 2018.

[16]. S.A.Chaudhry, M.T.Khan, M.K.Khan, and T.Shon, 'A Multiserver Biometric Authentication Scheme for SENSOR NETWORK using Elliptic Curve Cryptography',springer Journal of Cloud Systems, vol 40, pp: 230-243, Nov 2016.

[17]. C.T.Li,C.Y.Weng, and C.C.Lee, 'A secure RFID tag authentication protocol with privacy preserving in telecare medicine information system', springer Journal of Cloud Systems, vol 39, pp: 1–8, 2015.

[18]. M.Benssalah,M.Djeddou and K.DroPiche, 'Security Analysis and Enhancement of the Most Recent RFID Authentication Protocol for Telecare Medicine Information System', springer journal of Wireless Personal Communications pp: 6221–6238, vol 96, Oct 2017.

[19]. H.Lai, M.Luo,Z.Qu,F.Xiao, and M.A.Orgun, 'A Hybrid Quantum Key Distribution Protocol for Tele-care Medicine Information Systems', Volume 98, pp 929–943,Jan 2018.

[20]. Xie Q, Tang Z, Chen K. Cryptanalysis and improvement on anonymous three-factor authentication scheme for mobile networks. Comput Electr Eng 2017;59:218–30.

[21]. A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz, “Energy analysis of public-key cryptography for wireless sensor networks,” inThird IEEE International Conference on Pervasive Computing and Communications (PerCom), March 2005, pp. 324–328

[22]. V.Odelu,A.K.Das, and A.Goswami, 'An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card', Elsevier journal of Journal of Information Security and Applications, vol 21, pp: 1-19, 2015.

[23]. N.Druml,M.Menghin,A.Kuleta,C.Steger,R.Weiss,'A Flexible and Lightweight ECC-Based Authentication Solution for Resource Constrained Systems',17th Euromicro Conference on Digital System Design,2014.Italy.

[24]. M.Sarvabhatla,and C.S.Vorugunti, 'A Secure Biometric-Based User Authentication Scheme for Heterogeneous WSN',2014 Fourth International Conference of Emerging Applications of Information Technology, ISI-Kolkatta, 2015.

[25]. Q.Cheng,X.Zhang and J.Ma, 'ICASME: An Improved Cloud-Based Authentication Scheme for Cloud Environment', pp:41-44,March 2017.

[26]. S.I. Chu,Y.J.Huang and W.C.Lin, ‘Authentication Protocol Design and Low-Cost Key Encryption Function Implementation for

Wireless Sensor Networks',IEEE SYSTEMS JOURNAL, Vol 11, Dec 2017.

[27]. S.Kumari,X.Li,F.Wu,A.K.Das,H.Arshad, and M.K.Khan, 'A User Friendly Mutual Authentication and Key Agreement Scheme for Wireless Sensor Networks using Chaotic Maps', Vol 63, PP : 56-75, oct 2016.

[28]. V.Odelu, S.Banerjee, A.K.Das, S.Chattopadhyay, S.Kumari,X.Li and A.Goswami, 'A Secure Anonymity Preserving Authentication Scheme for Roaming Service in Global Mobility Networks',springe journal of Wireless Personal Communications, vol 96, pp: 2351–2387,sep 2017.

[29]. V.C.Sekhar, M.Bharavi, A.Ruhul, P.B.Rakesh, and S.Mrudula, 'Improving Security of Lightweight Authentication Technique for Heterogeneous Wireless Sensor Networks',springer journal of Wireless Personal Communications, pp:1–26,2017.

[30]. X.Li,F.Wu,M.K.Khan,L.Xu,J.Shen and M.Jo, 'A Secure Chaotic Map-based Remote Authentication Scheme for Telecare Medicine Information Systems.',elsevier journal of Future Generation Computer Systems, Aug 2017.

[31]. A.Chaturvedi, D.Mishra, S.Jangirala and S.Mukhopadhyay, 'A privacy preserving biometric-based threefactor remote user authenticated key agreement scheme.',Elsevier Journal of Information Security and Applications, Vol 32

Cite this article as :

P. Lokesh Kumar Reddy, Dr. K. Ramesh Reddy, "Critical Security Mechanism Designed for Data Transmission in Wireless Sensor Networks using Hierarchical Cloud Server", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 117-129, March-April 2019. Available at doi : https://doi.org/10.32628/CSEIT195214
Journal URL : http://ijsrcseit.com/CSEIT195214