Int. j. inf. tecnol. (March 2023) 15(3):1221–1230
https://doi.org/10.1007/s41870-023-01173-2

ORIGINAL ARTICLE

An efficient Key Agreement and Authentication Scheme (KAAS) with enhanced security control for IIoT systems

G. Umarani Srikanth[1] · R. Geetha[2] · S. Prabhu[2]

Received: 21 August 2022 / Accepted: 1 February 2023 / Published online: 11 February 2023

Abstract Internet of Things is one of the prevalent and inevitable trends of the current era where data is found to be scattered among sensing devices. This paper addresses about preserving the privacy and security of the data that is distributed among the sensors collected by the users in Industrial Internet of Things infrastructure domain. This work adopts a dynamic authentication key agreement strategy which permits authenticated users to access the data which is distributed among various IoT sensing devices. In the proposed work an efficient Key Agreement and Authentication Scheme is designed to ensure the establishment of secure data communication. The model called Real-or-Random and tool named Automated Validation of Internet Security Protocols are deployed to ensure the secured transmission of data collected by innumerous sensors deployed across the network. Scaling of the network is done by addition of new nodes followed by pre-deployment phase and restoration of the transmission route is done effectively if any intrusion is found. The performance of the scheme is validated by measuring the parameters such as throughput, residual energy, packet dropping rate and delay analysis and it is found that the proposed scheme is superior compared with existing schemes.

Keywords Security · Authentication · Wireless sensor networks (WSNs) · Industrial Internet of Things (IIoT)

✉ R. Geetha
geetha@saec.ac.in

[1] Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, India

[2] Department of Computer Science and Engineering, S.A. Engineering College, Chennai, India

1 Introduction

IoT becomes one of the rapid growing and remarkable technologies as it makes the sensors and objects get connected with each other over the internet. The internet has challenges in ensuring privacy and security of the data collected by devices which demand the public attention over the years. The challenges in terms of user's authentication, scaling the network, handling technical issues and adopting new policy are being solved as of now. The IoT devices need subtle human interaction and produces huge volume of data. The market trends have brought the IoT into widespread reality which includes surge of techniques in data analytics, general adoption of miniaturization, IP-based networking and global connectivity among the sensors that produces data stored in cloud[1]. The implementation of IoT mainly depends upon the most commonly used technical communications models: Device-to-Cloud, Device-to-Device, Device-to-Gateway and Back-End Data-Sharing.

All these communication modes are more flexible in providing IoT devices communicated among themselves and provide valuable data to the user. It has a huge craze in digital market and rule the globe in the upcoming years. IoT can be viewed as a giant and smart network, connects things and people, collects data and share them between the things by the way they are programmed. It witnesses general-purpose nature of the web service architecture that does not have constraints on applications to use the technology. Safety and resilience of the web are affected if a less secured device is connected online. This drawback is amplified into the considerations like deployment of homogenous IoT devices in a mass-scale. IoT deals to retrieve the data in the public channel that can be either lost or stolen and implements increased tracking, surveillance of data, data collection and gathering the data streams collected over the internet which can be

termed as digital portraits of users. The challenges like user authentication and governance are wide and sophisticated in nature, have to be addressed.

The IIoT [2] is termed as a collection of sets of smart sensors and objects which are interconnected with real time industrial applications setup. The connectivity also deals with data aggregation, exchange and big data analysis. This in turn enhances the outcome such as productivity of data with the deployment of cloud. The IIoT has been considered to represent a parallel and distributed system which ensures high degree of automation of the monitoring and control of physical infrastructures in association with cloud infrastructure [3]. The other technologies such as cyber security, edge computing, mobile technologies, machine-to-machine communication, 3D printing, advanced robotics, bigdata, RFID technology and cognitive computing are also associated with IIoT.

The cyber-physical system is the enabler for establishing the communication over connected physical machines in the presence of IoT and IIoT environments. Moreover cloud computing domain facilitates establishing the connection among storage devices in cloud where files and data can be kept and retrieved. Accessing these stored files made easier as they are being stored in cloud instead of our local storage devices. Edge computing [4] is considered as a process in which decentralization of data is achieved at the edge of the network. In order to achieve incredible improvements in terms of accessing the huge volume of data and productivity across the users in the industrial applications, the IIoT requires edge-plus-cloud architecture. Big data analytics [5] is also adopted to investigate and analyze the data sets. Human anthropology can be achieved with the help of artificial intelligence [6] in which powerful algorithms and models are designed to help humans to take correct decisions during the analysis of data. The different layered modular architecture in the digital technology environment is referred to as IIoT systems. This includes some important physical components like cyber physical system, machines and sensors [7]. These components require to adopt the secure communication [8] strategies among them.

The rest of the paper is presented as follows. In chapter 2 the survey related to proposed work is discussed. Chapter 3 discusses about authentication and key agreement schemes. In chapter 4 the simulation results are presented and discussed. At the end, proposed work is concluded.

2 Related work

The authors in the paper [9] have presented a new strategy to address the privacy in the context billing under dynamic electricity pricing. The bi-directional communication between user and smart grid tend to face security and privacy issues[10] were addressed. In order to resolve the security constraint, proposed scheme introduces an efficient data aggregation scheme for executing the privacy-friendly price-based billing. This scheme consists of three phases of security such as authenticated initialization and refilling, data aggregation for price-based billing and demand response. These methods ensure the user privacy information when smart grids are subjected to capture fine-grained energy usage information. Moreover, from the empirical results it was found that proposed method achieves better privacy protection for electric meter reading aggregation and feasible computational efficiency. The authors of this paper [11] have presented a novel user authentication protocol which can be deployed in a resource constrained WSN protocol in order to solve user authentication issues. It is an ECC based protocol which uses an overall handshake module to solve the challenges. DES encryption algorithm was deployed for providing authentication among users, gateway and IoT devices and also used for generating session key. Furthermore, from the experimental results, it was found that this protocol escalates the security analysis by using ECC-based protocol in WSNs.

In the research work [12], the authors discussed about patient information and health care management in IoT environment. This work proposed a secure IoT based health care monitoring system using body sensor networks which provides major security requirements in modern health care system. The system also allows the integration of intelligent, miniaturized, low-power body sensor nodes in and around the body to monitor the body functions and surrounding. The proposed scheme provides security to the sensor nodes against data privacy, data integrity, data freshness, anonymity and authentication. The proposed research work ensured that the scheme was light-weight in nature computationally feasible. In the article [13] the authors have presented a method called smart card based authentication can be applied in heterogeneous wireless ad-hoc sensor networks. This proposed scheme was proved to be more efficient in resolving several attacks such as impersonation attacks, stolen smart card attacks, node spoofing[14] attacks, etc. The proposed scheme uses hash function and XOR operation for authentication and it provides backward secrecy against the node spoofing attack. Also it was proved to solve the Elliptic Curve Discrete Logarithmic problem and found to enhance authentication using forward secrecy. The authors found that the proposed work provides greater security for protecting the password[15] which is mandated in WSNs where these networks demands highest degree of security using passwords.

A novel authentication protocol to be handled in wireless sensor networking system using ECC was proposed [16]. This work applied the ECC and a user authentication protocol to authenticate the clients. The author used a gateway

node for applying three-way handshake mechanism. The gateway node acts as intermediate node between user and the IoT sensing devices. From the results the authors found that this ECC based authentication protocol was found to be more suitable for achieving high security in WSN networks. In [17] the authors have focused on Hierarchical IoT Networks which consist of different nodes namely gateway node, cluster head node and sensing node organized in a hierarchy. This paper emphasizes on the design of a new secure lightweight three-factor remote user authentication scheme for the hierarchical IoT networks called the User Authenticated Key Management Protocol which uses three key factors namely passwords, smart cards and personnel bio-metrics. Using this scheme, a user can access the real time data from the sensing nodes with good authentication strategy. The proposed scheme provides offline sensing node registration, freely password, user anonymity and bio-metric update facility. Empirical results have proved that the proposed work provided better computation and communication costs.

Resource constrained problem of the sensor nodes were thoroughly analyzed in [18] and authors proposed a 3-factor anonymous authentication scheme for WSNs. This proposed scheme uses a fuzzy commitment scheme for biometrics environment. The fuzzy scheme emphasizes the three-way handshake protocol and provides authentication to the user and the gateway. From the results it was observed that proposed scheme solved the problem design, security and efficiency of WSNs and improved the computational efficiency. It also achieved higher security, more functional requirements and seems to be suitable for high security WSN networks. The authors [19] focused on the security issues encountered during the bi-directional communication between the smart grids and service providers. They proposed a privacy-aware key agreement scheme for smart grid communication which deployed the lightweight cryptographic primitive such as the Physically Unclonable Function to protect the smart grid from hardware related security issues. In order ensure security and establish reliable communication, the proposed scheme utilized one-way hash function that encrypts data and session key. From empirical results it was shown that the proposed scheme was computationally feasible, cost efficient and can be adopted in resource-constrained smart meters.

The authors highlighted the password authentication of the WSNs in the IoT environment [20]. They proposed a one way function protocol, where the gateway node provides encryption between user and IoT sensing devices. It also resolved security and privacy issues, protects itself from illegal access of intruders. This one-way function protocol also encodes the password by encrypting the master keys and providing session keys during transmission. The user's password was encrypted and validated by the system. From the experimental results it was found that this protocol provides greater security and privacy for password and is found to be suitable for WSN network. IoT in e-healthcare was discussed [21] where a new remote user authentication protocol for enhancing e-healthcare process was presented. The remote user protocol is based on extended chaotic maps that permits only authorized users to access the medical server data via wireless communication. The gateway node acts as a trusted node, provides authentication to the user. It was found from result that this scheme avoids computational expenses, secure and practical for battery limited devices and suitable for high security wireless communication.

The authors have highlighted a new authentication scheme [22] for accommodating medicine anti-counterfeiting system that can be adopted in IoT environment. It was designed for examining the authenticity of pharmaceutical products used. It uses Near Field Communication in mobile environment and generates a session key which is robust against known attacks. From the empirical results it was observed that this scheme lowered the computation and communication cost, provided additional functionality features suitable to be used in WSN. In this paper [23] the authors have focused the wireless sensor nodes where integrity and trustworthiness of the nodes are taken as the key aspects. A novel zero watermarking scheme was proposed that accepts captured data from the surrounding vicinity and produces different watermarks as required. These watermarks are generated using the data length. From the results it was found that the proposed scheme can withstand multiple attacks on data and withstand attacks against various watermarks such as data deletion, data modification and data duplication. It was also found that proposed scheme is light-weight in nature, computationally efficient and reliable.

The authors in [24] proposed a lightweight privacy-preserving authentication protocol for RFID systems that uses a Physically Unclonable Functions to rectify security issues by encrypting RFID tags. It initiates three-way handshake protocol scheme for providing authentication and security to RFID systems thereby reducing computational cost. The experimental results have shown that this work provides secured data communication, efficient, suitable to be used with resource-constrained RFID tag. Authentication and security in WSNs was addressed in [25], which deployed a temporal-credential- based two factor authentication scheme using the Elliptic curve cryptography. Three-way handshake adopted where the user and IoT sensing devices are provided secret keys for transmission of data. Gateway node acts as a trusted node which does data encryption by generating a secret key and from results it was observed that this scheme can resist a variety of attacks such as personification attack, smart card attack etc., and it provides various security features. The related work is consolidated and shown in Table.1.

Table 1 Overview of the related work

Article	Issues addressed	Proposed scheme	Results arrived
[9]	Privacy in the context billing under dynamic electricity pricing	Efficient data aggregation scheme	User privacy information was achieved
[11]	User authentication issues	ECC based protocol	Improved security in WSNs
[12]	Patient information and health care management in IoT environment	Secure IoT based health care monitoring system	Security to the sensor nodes against data privacy, data integrity, data freshness, anonymity and authentication
[13]	Various types of attacks exist in WSNs	Smart card based authentication applied in heterogeneous wireless ad-hoc sensor networks	Greater security for protecting the password which is mandated in WSNs
[16]	Authentication of clients	ECC and a user authentication protocol to authenticate the clients	High security in WSN networks
[17]	Remote user authentication	New secure lightweight three-factor remote user authentication scheme	Better computation and communication costs
[18]	Resource constrained problem of the sensor nodes	Fuzzy commitment scheme for biometrics environment	Security and efficiency of WSNs and improved the computational efficiency
[19]	Security issues encountered during the bi-directional communication between smart grids and service providers	Privacy-aware key agreement scheme for smart grid communication	Feasible, cost efficient and can be adopted in resource-constrained smart meters
[20]	Password authentication of WSNs in the IoT environment	One-way function protocol	Greater security and privacy for password achieved
[21]	IoT in e-healthcare	New remote user authentication protocol for enhancing e-healthcare process	Avoids computational expenses, secure and practical for battery limited devices
[22]	Authenticity of pharmaceutical products used	Near Field Communication in mobile environment	Lowered computation and communication cost
[23]	Integrity and trustworthiness of the nodes	Novel zero watermarking scheme	Light-weight in nature, computationally efficient and reliable
[24]	User authentication in RFID systems	Lightweight privacy-preserving authentication protocol for RFID systems	Secured data communication, efficient
[25]	Authentication and security in WSNs	Temporal-credential- based two factor authentication scheme using the Elliptic curve cryptography	Can resist a variety of attacks such as personification attack, smart card attack etc

The work in this paper addressed the secure authentication mechanism that can be established between user and IoT devices using gateway Key Agreement and Authentication Scheme. Declaration of the nodes, pre-establishment of the network, the process of user registration, key authentication and dynamic IoT sensing device phases are designed. The relay attack has been overcome with the help of timestamps which makes all nodes in the network become synchronized with users, gateway nodes and IoT sensing devices. Before installation of IoT sensing Nodes in the IIoT environment, it is loaded with the credentials. The nodes are mutually authenticated with each other in the login and authentication phases, then secret key is said to be shared among them ensure secure communication. If a registered user node is willing to update the key dynamically it can be processed through KAAS. Interestingly, this Dynamic Authentication Key Agreement Scheme is completely executed with the help of the gateway Node with the credentials of other genuine nodes. The revocation process becomes useful if a legal node credentials is lost or stolen and it is done with the help of Effective Path Selection and Security Control Logic scheme. Finally, the dynamic IoT sensing device phase is designed to deploy some additional IoT nodes in the network. This proposed work is primarily aimed to have a secure and faster authentication scheme that can used to transfer data in a much more secure way than that of the existing authentication schemes with minimal loss, rerun of network deployment is less, efficient network lifetime management and condensed intrusion attacks [26].

3 Proposed work

There are different phases involved in the proposed model as shown in Fig. 1. The first phase called network establishing phase initiates the mounting of computational nodes which are programmed with all intended credentials. The gateway node is identified and intended to generate the secret key. Scaling of the network can be done by adding some additional nodes dynamically. Agreement

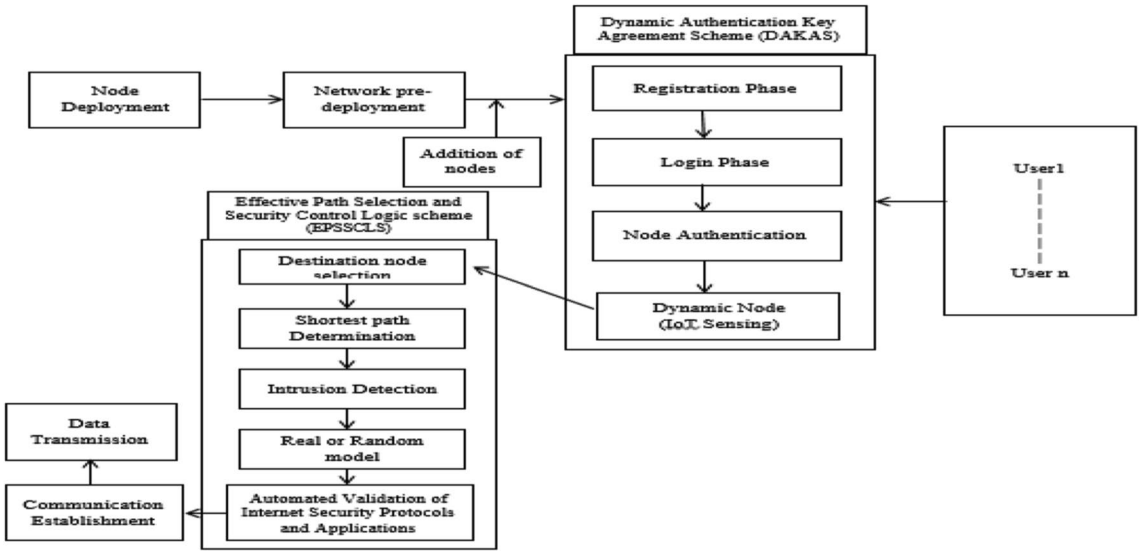


Fig. 1 Phases of the proposed model

and authentication scheme is well designed which has four phases called registration phase, login phase, authentication phase and dynamic node sensing. The first phase is designed to have three stages namely creation of user login ID, password and biometrics. The gateway node creates user's secret key to be known to authenticated client and gateway node. The login phase enables creating login for user using smart card and chooses the appropriate IoT sensing device. The authentication phase examines the origin of the message using timestamp. Verification phase examines the secure communication channel established among user to gateway and gateway to IoT sensing device. Dynamic node sensing phase is meant for verifying the authentication of the user and their connected IoT devices. Mutually they share a common session key to initiate the session followed secure data transmission. The next component is Effective Path Selection and Security Control Logic scheme where it has phases like destination node selection, shortest path determination, intrusion detection, Real-Or-Random model and Automated Validation of Internet Security Protocols and Applications. The target computational node is then found to where the secured data has to be directed and shortest route is said to be identified with the help of relay nodes. Intrusion detection is said to be achieved to find intruder or unauthorized users who try to access aggregated data in the network. If the source node doesn't receive the acknowledgement message at the stipulated time, it is understood that the intruder has been detected and destination path is altered. The formal security verification is executed using Real-OR-Random model and Automated Validation of Internet Security Protocols and Applications(AVISPA) tool. Then communication establishment phase is used to establish communication between the nodes to enable data transmission to be taken place in the network as shown in Fig. 1.

Intrusion or spoofing can be detected without human intervention. Dynamic distributed key infrastructures and identity based protocol was deployed to ensure verification and authentication of network users, requires some important parameters like one-time-pad encryption, secure network access, digital signature, Digital Rights Management(DRM), repudiation, authentication, revocation and authorization used in digital context. A single key can be used to address all security needs. The most secure systems are network topologies in which users are pre-authenticated and keys are pre-distributed to all network users. This eliminates the problems faced during key exchange occurred in network sessions.

As stated, the level of secure authentication starts from the node level. the nodes are mutually authenticated with each other in the login and authentication phases and then session key (i.e. shared secret key) among them is established to communicate securely. The scope of the research work is to provide a secure and faster authentication scheme that can used to transfer data in a much more secure way than existing authentication schemes. The necessary notations and their descriptions are shown in Table 2.

3.1 Registration phase

In the registration phase of the process as shown in Fig. 2, the User (U_i) has to register with the Gateway Node in an offline mode via a definitive channel. The important steps are illustrated as follows:- U_i has to select his/her identity $\mathbf{IDR_i}$, password $\mathbf{PSD_i}$, and generate some random numbers a_i, P_i, P_j, n_{i1}, n_{i2}. U_i then computes $DIDR_i = h(IDR_i || a_i)$

Table 2 Notations and description

Notations	Description	Notations	Description	Notations	Description
GTN	Gateway Node	^TD	Transmission Delay	SIN_j	ID of Nodes
ISN_j	IoT Sensing Node	Grt(.)	Fuzzy extractor generator	a_i, p_i, p_j, $n_{i1,}$ n_{i2}	Random Numbers
U_{rj}	User	Rpd(.)	Fuzzy extractor reproducer	TSt1, TSt2, TSt3	Timestamp
X_{GTN}	Master Secret Key	T_p	Threshold parameter	C_n	Smart card code
St_{key}	Secret Key between Gateway node and IoT sensing node	$P_n(x)$	Chebyshev Polynomial of Degree	SR_i	Smart card
X_{GTN}—U_{rj}	Secret Key between User & Gateway node	(+)	Bitwise exclusive OR	PSD_i	Password
IDR_i	ID of user i	h()	Hash function	||	Concatenation operator

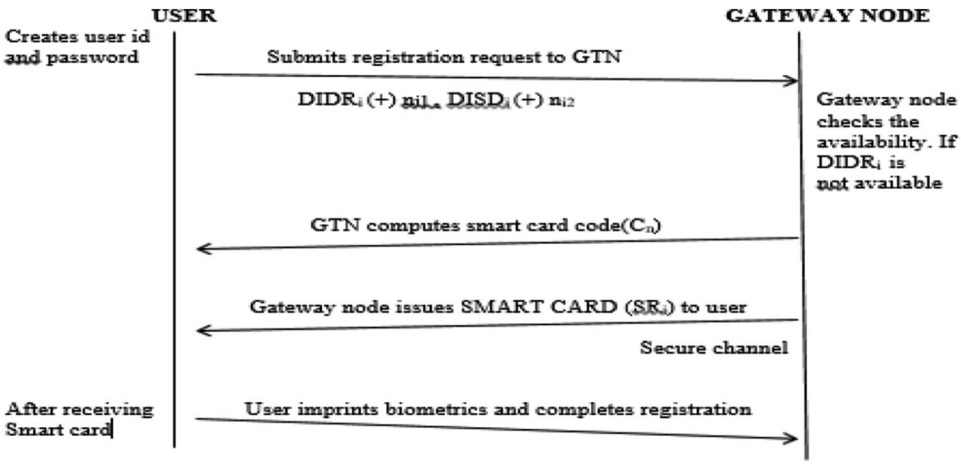


Fig. 2 Sequence of registration phase

and $DPSD_i = h(IDR_i||PSD_i)$, and submits the registration request $DIDR_i \_ n_{i1}$; $DPSD_i \_ n_{i2}$ to the registered Gateway Node securely. The importance of using this random secrets n_{i1} and n_{i2} here is to protect from privileged-insider attack in the scheme. Even if an authorized user of the gateway node is the insider attacker knows the information, without having this random secrets, it will be difficult and practically infeasible to find the same ID and passwords $DIDR_i$ and $DPSD_i$. Therefore, the attacker does not have the knowledge of secrets IDR_i and PSD_i. After receiving the request, the Gateway Node will check the availability of $DIDR_i$ in its database. If $DIDR_i$ is not available, the Gateway Node calculates according to the Eq. (1)

$$C_n = DIDR_{i\_}\, n_{i1}.\, DPSD_{i\_}\, n_{i2}.\, h(X_{GTN}||\, h(X_{GTN}(+)\, U_i)) \quad (1)$$

The GTN then issues a smartcard SR_i to U_i secretly. After receiving SR_i, U_i marks his/her biometrics BM_i of a specific terminal or mobile device in its sensor.

$E_i = h(J_i \,\|\|\, h(\_i \,\|\| PSD_i) \,\|\| TS_1)$	$E0_i = E_{i\_}h\ (DIDR_i \,\|\| J_i \,\|\| TS_1)$,
$A_g = T_{ri}\ (DIDR_i \,\|\|\, SIDR_j \|\|\, E_i)$	$DIDR_{0i} = DIDR_{i\_}\, h(E_i \,\|\| J_i \,\|\| TS_1)$
$G_i = A_{g\_}\, h(DIDR_i \,\|\| J_i \,\|\| TS_1)$	and
$V_{GTN} = h(DIDR_i \,\|\| A_g \,\|\| G_i \,\|\| SIDR_j \,\|\| TS_1)$	$SID0_j = SIDR_{j\_}\, h\ (DIDR_i \,\|\| TS_1)$ and computes Gen (BM_i)

3.2 Login and authentication phase

The sequence of operations performed in login and authentication phase is shown in Fig. 3. In this phase the login activity is executed with the help of a user U_i as mentioned in the following steps.

L1: First, user U_i uses his/her smart card SR_i and then inserts the same into the reader by giving the login authentication credentials, user id IDR_i and password PSD_i. Then the user places his biometrics BM_i. Then SR_i then finds $DPSD_i = h(IDR_i \,||PSD_i)$ and checks if $RB_i = h(IDR_i||PSD_i)$.

L2: If the above test is completed successfully and noted as satisfied, then SR_i assures that U_i's entered credentials

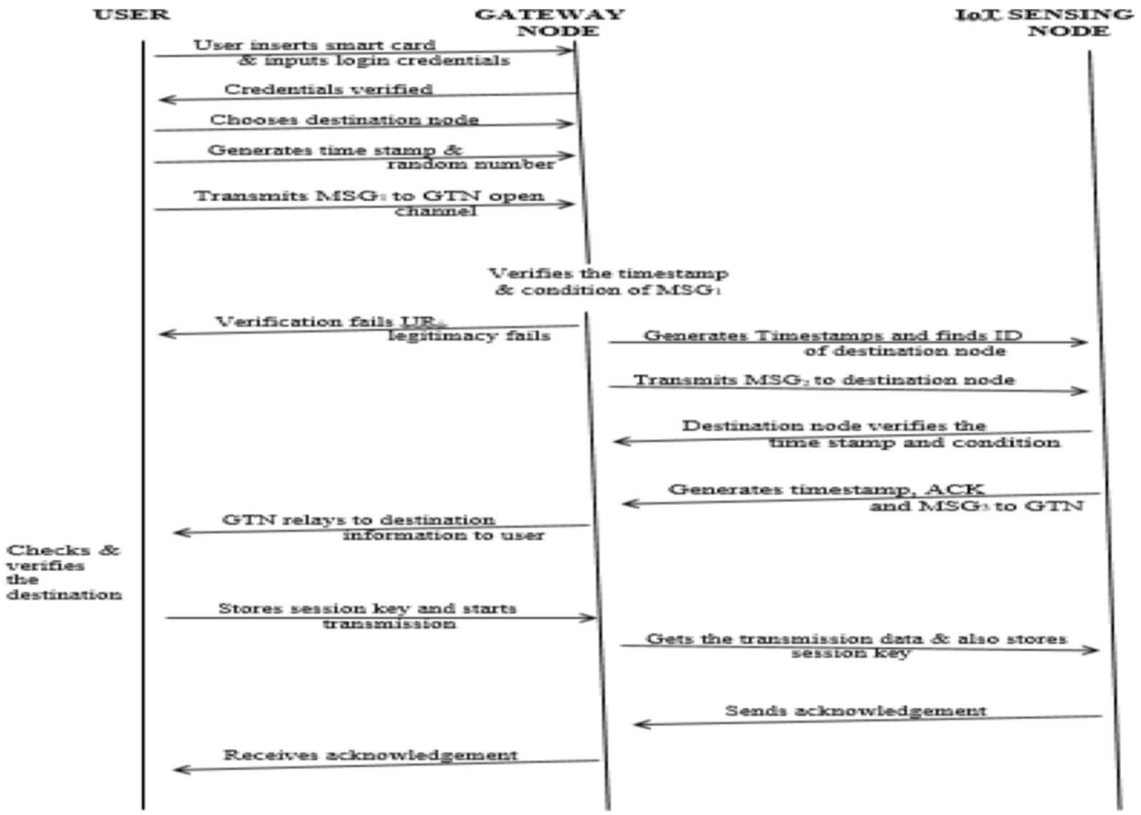


Fig. 3 Login and authentication phase

(IDR_i; PSD_i; BM_i) are true, and then finds $C_n = C0_n\_h(i \| IDR]_i)$, $DIDR_i = h(IDR_i \| a_i)$, $J_i = C_n\_ DIDR_i\_ DPSD_i$ with its stored parametric conditions. In this step, U_i then picks the ID, $SIDR_j$ of an used IoT sensing device ISN_j from which he is willing to avail the services.

L3: Then SR_i produces current timestamp TS_1 and random number r_i. Finally the login message is transmitted to the gateway over an open channel as follows. $MSG_1 = \{E0_i; DIDR0_i; V_{GTN}; Gi; SID0_j; TS_{1g}\}$. So far, the interaction between the user and gateway was shown. The following steps are activities that are required to complete this phase:

A1: After receiving the message MSG_1 (Transmitted Message by the user U_1) from U_i, the Gateway Node calculates the message freshness with the help of the condition $|TS0_1\_TS_1| <\_T$, where the transmission delay is denoted as _T and the received time message is $TS0_1$. If the condition is evaluated to be true, the GTN then computes the following:

$M_i = h(X_{GTN} \| h(X_{GTN} \| U_i))$,

$DIDR_i = DIDR0_i\_ h(E0_i \| M_i \| TS_1)$,

$A_g = G_i\_ h(DIDR_i \| M_i \| TS_1)$,

$SIDR_j = SID0_j\_ h(DIDR_i \| TS_1)$, and verifies the condition.

$V_{GTN} = h(DIDR_i \| A_g \| G_i \| SIDR_j \| TS_1)$.

A2: If the above condition fails, the Gateway Node (GTN) rejects the right of the User by not accepting the login message MSG_1. Otherwise, the Gateway Node(GTN) computes $E_i = E0_i\_ h(M_i \| DIDR_i \| TS_1)$ and also generates current timestamp TS_2.

A3: On receiving MSG_2, ISN_j (IoT Sensing Device) later calculates the message freshness with the help of the condition $|TS0_2\_TS_2| <\_T$, where the receiving time of the message is $TS0_2$. If the result of checking holds true, ISN_j also checks the condition $VSN_j = h(S_{keyj} \| SIDR_j \, kA0_g \| h_j \, kTS_2)$. If the condition fails, IoT sensing Device rejects MSG_2.

A4: Then the ISN_j produces a random number r_j with present timestamp TS_3, and then calculates.

$N_j = T_{rj} (DIDR_i \| SIDR_j \| E_i)$,

$S_{ij} = h(T_{rj} (A0_g) \pmod p \| DIDR_i \, kTS_3)$ as the session shared between U_i and ISN_j,

$P_j = h(S_{Kij} \| N_j \| TS_3)$ and $N0_j = N_j\_ h(DIDR_i \| SIDR_j \, kTS_3)$.

ISN_j then transmits the message $MSG_3 = f_{Pj}; N0_j; TS_{3g}$ to U_i via the open channel.

A5: Finally U_i receives the message MSG_3 and calculates the message freshness with the help of the condition $|TS0_3 \| TS_3| <\_T$. If the result of this checking holds true, then SR_i again computes $N_j = N0_j\_ h(DIDR_i \| SIDR_j \, kTS_3)$ and the session key.

if the verification holds, U_i authenticates ISN_j. Atlast, U_i and ISN_j will store the common session key 'r' shared secret key $S_{Kij} = (SK_{ij})$ for their forthcoming secure communication.

4 Results and discussion

The result of the proposed work is demonstrated using NS2 simulator. In this work, our demonstration is mainly focused on network throughput performance and end-to-end delay analysis which has a major impact on the Dynamic Authentication Key Agreement Scheme. The important parameters like throughput, residual energy, packet dropping rate, delay analysis are measured and represented in a graphical format. It is compared with the existing systems.

4.1 Throughput analysis

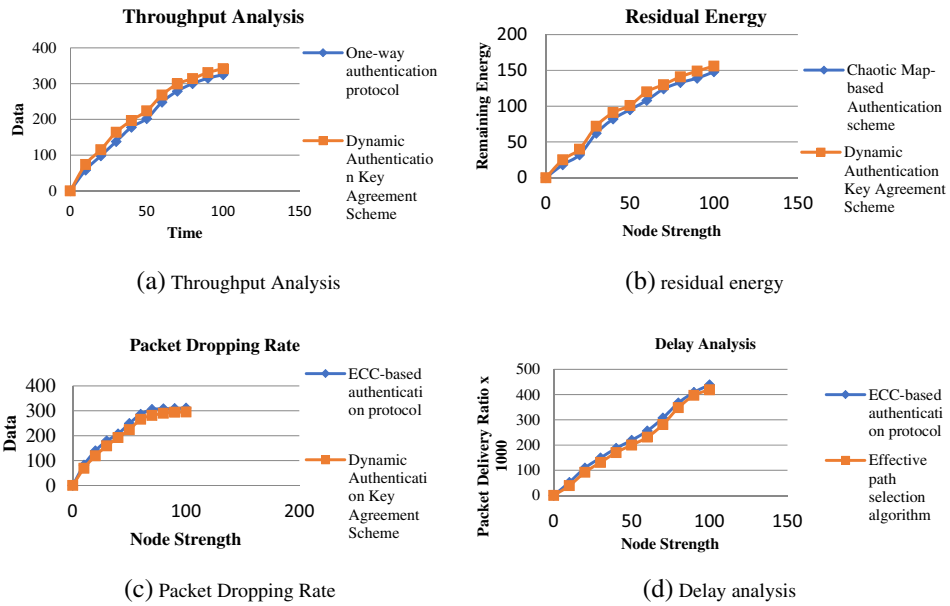
The network throughput is considered as an important performance parameter in the network which can be defined as the total number of bits transmitted in unit time, and it is formally calculated as $(\_r \_ j \_j) = T_d$, where T_d is the maximum time taken (in seconds), _j the amount of data (size of a packet), and _r is the number of received packets during transmission as shown in Fig. 4a. The actual total time is taken as 100 s, which is basically referred as simulation time. Throughput is calculated as shown in Fig. 4a with time in the x-axis and data in the y-axis. Throughput of Dynamic Authentication Key Agreement Scheme is comparatively less than the one-way authentication protocol, because our scheme makes use of less-sized messages during the login & authentication phases. However, the scheme provides good security and greater functionality features.

4.2 Residual energy

Residual energy plays a vital role in determining the energy of nodes after transmission. It is defined as energy left in the particular node after the completion of transmission or reception of routing packets. Nodes will make use of energy for transmission or reception of routing packet and therefore it may lose energy. The resulted value i.e. initial Energy of a particular node may get decreased. The residual energy can be utilized to find the estimated time during transmission or reception. The residual energy E_n is calculated by dividing the current consumption in per component to duty cycle T_n, which were obtained to estimate the usable time. Residual energy is calculated with node strength in the x-axis and remaining energy in the y-axis. As shown in Fig. 4b, it is observed that the residual energy of nodes in the Dynamic Authentication Key Agreement Scheme is comparatively greater than the Chaotic Map-based Authentication scheme. The proposed scheme provides low power consumption and greater battery life to the nodes in the network.

4.3 Packet dropping rate

Packet dropping rate is one of the factors that determines the reliability of the IoT sensing devices. It is defined as the rate of loss in the transmission of data packets. The packet loss is calculated as a percentage of packets lost with respect to packets sent. The retransmission of packets should also be considered. It is caused by errors in data transmission; typically across wireless networks or network congestion. So the proposed scheme initiates an Effective path selection algorithm to securely transmit data without causing much data loss. Packet dropping rate is calculated with node strength in the x-axis and data in the y-axis. The graph shown in Fig. 4b screens that the Dynamic Authentication Key Agreement Scheme has less packet dropping rate when compared to the ECC-based authentication protocol. The proposed scheme



(a) Throughput Analysis

(b) residual energy

(c) Packet Dropping Rate

(d) Delay analysis

Fig. 4 **a** Throughput analysis. **b** Residual energy. **c** Packet dropping rate. **d** Delay analysis

also provides speculation in the dropping rate and provides reliable communication among IoT sensing devices.

4.4 Delay analysis

It is understood that delay performance is key parameter for every successful development and deployment of all the real-time networked sensing applications. End-to-End delay refers to the total amount of time taken for a packet to transmit across the network from source to destination. The particularity of the sensing scenario is that all nodes generate and collectively work together to stimulate transmission at a higher rate. Delay is calculated with node strength in the x-axis and packet delivery ratio in the y-axis. The proposed scheme is verified through comparison between the analytical and numerical stimulated result and the graph shown in Fig. 4d is used to conclude that the Dynamic Authentication Key Agreement Scheme provides less transmission delay compared with ECC-based authentication protocol.

5 Conclusion

The Dynamic Authentication Key Agreement Scheme proposed in this research work found to be scalable and efficient in achieving better authentication between the sensor nodes in an IIoT environment. The scheme supports both static and dynamic IIoT wireless sensor nodes, provides secure and authenticated communication between any pair of nodes. Node compromising attacks are resilient and scalable and the capacity of managing the revocation list for lost nodes or compromised nodes is found to be fair. The work was carried out and compared with some popular and latest protocols where are used in WSNs. This scheme also proves to be efficient in saving the energy with minimum of 20% in communication. Further, this scheme makes use of less memory cost and provides higher probability in sharing a secret key between two sensor nodes.

Funding No funding.

Declarations

Conflict of interest No Competing interest.

References

1. Geetha S (2020) Umarani : cloud integrated IoT enabled sensor network security: research issues and solutions. Wireless Pers Commun 113:747–771
2. Xiangwang H, Zhiyuan R, Kun Y, Chen C, Hailin Z, Yao X (2019) IIoT-MEC: a novel mobile edge computing framework for 5G-enabled IIoT
3. Tessema M, Abdulrahman A, Abdullah A, Yousef A, Dunren C (2017) A no data center solution to cloud computing. In: IEEE 10th International Conference on Cloud Computing. pp. 714–717
4. Kai F, Qiang P, Junxiong W, Tingting L, Hui L, Yintang Y (2018) Cross-domain based data sharing scheme in cooperative edge computing. In: IEEE International Conference on Edge Computing. pp. 87–92
5. Alka L, Rao P (2017) Platforms for big data analytics: trend towards hybrid era. In: International Conference on Energy, Communication, Data Analytics and Soft Computing. pp. 3235–3238
6. Ahmad AS, Sumari AD (2017) Cognitive artificial intelligence: brain-inspired intelligent computation in artificial intelligence. In: Computing Conference, 135–141
7. Geetha M (2019) Padmavathy, lallithasree: a light weight secure communication scheme for wireless sensor networks. Wireless Pers Commun 108:1957–1976
8. Geetha P (2020) Thilagam, lallithasree : tamilian cryptography: an efficient hybrid symmetric key encryption algorithm. Wireless Pers Commun 112:21–36
9. Gope P, Sikdar B (2018) An efficient data aggregation scheme for privacy-friendly dynamic pricing-based billing and demand-response management in smart grids. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2018.2833863
10. Mishra N, Shahid HM, Tripathi JP (2015) A compendium over cloud computing cryptographic algorithms and security issues. BIJIT—BVICAM's International Journal of Information Technology. Vol. 7 Ndrseco. 1; ISSN 0973–5658
11. Yeh H-L, Chen T-H, Liu P-C, Kim T-H, Wei H-W (2011) A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. Sensors 11(5):4767–4779
12. Gope P, Hwang T (2016) BSN-care: a secure IoT-based modern healthcare system using body sensor network. IEEE Sensors J 16(5):1368–1376
13. Chang C-C, Le H-D (2016) A provably secure, efficient and flexible authentication scheme for Ad hoc wireless sensor networks. IEEE Trans Wirel Commun 15(1):357–366
14. Pandey A, Saini JR (2017) Comprehensive security mechanism for defending cyber attacks based upon spoofing and poisoning. BIJIT—BVICAM's Int J Inf Technol. 8(2). ISSN 0973–5658
15. Sriharsha B, Zabiullah, Vishnu S B, Sanju V (2016) Password protected locking system using arduino. BVICAM's Int J Inf Technol. 8(1). ISSN 0973–5658 959
16. Shi W, Gong P (2013) A new user authentication protocol for wireless sensor networks using elliptic curves cryptography. Int J Distrib Sensor Netw. 2013:1–7
17. Wazid M, Das AK, Odelu V, Kumar N, Conti M, Jo M (2018) Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet Things J 5(1):269–282
18. Li X, Niu J, Kumari S, Wu F, Sangaiah AK, Choo K-KR (2018) A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. J Netw Comput Appl 103:194–204
19. Gope P, Sikdar B (2018) Privacy-aware authenticated key agreement scheme for secure smart grid communication. IEEE Trans Smart Grid. https://doi.org/10.1109/TSG.2018.2844403
20. Lamport L (1981) Password authentication with insecure communication. Commun ACM 24(11):770–772
21. Roy S, Chatterjee S, Das AK, Chattopadhyay S, Kumari S, Jo M (2017) Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing internet of things. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2017.2714179
22. Wazid M, Das AK, Khan MK, Al-Ghaiheb AAD, Kumar N, Vasilakos AV (2017) Secure authentication scheme for medicine anti-counterfeiting system in IoT environment. IEEE Internet Things J 4(5):1634–1646

23. Hameed K, Khan A, Ahmed M, Reddy AG, Rathore MM (2018) Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks. Future Gener Comput Syst. 82:274–289
24. Gope P, Lee J, Quek TQS (2018) Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. IEEE Trans Inf Forensics Secur 13(11):2831–2843
25. Jiang Q, Ma J, Wei F, Tian Y, Shen J, Yang Y (2016) An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. J Netw Comput Appl 76:37–48
26. Beigh BM (2015) Framework for choosing best intrusion detection system. BIJIT—BVICAM's Int J Inf Technol. 7(1); ISSN 0973–5658 821