FOREX Publication
Open Access | Rapid and quality publishing

International Journal of
Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 4 | Pages 1030-1038 | e-ISSN: 2347-470X

An Enhanced Authenticated Key Agreement Scheme for Cloud-Based IoT in Wireless Sensor Networks

Sartaj Singh[1] and Amar Singh[2]
[1,2] *School of Computer Applications, LPU Phagwara, sartaj_2292@yahoo.com[1], amar.23318@lpu.co.in[2]*

***Correspondence:** Sartaj Singh; sartaj_2292@yahoo.com

ABSTRACT- Recent advancements in mobile and wireless technology have fundamentally impacted the underpinnings of cloud computing and IoEs. These changes have changed the way data is communicated across numerous channels, allowing for intelligent discovery and operation. The Internet of Things (IoT) is highly reliant on wireless sensor networks (WSNs), which have several applications in industries ranging from smart medicine to military operations to farming. The IoT's substantial reliance on these activities generates a large amount of data. All the above-specified data is transferred to a remote server for storage and processing. As a result, it is critical to enable safe data access in WSNs by authenticating individuals in altered states of awareness. Authenticating drug addicts in WSNs is still a topic that has not been fully addressed. This study describes a novel and improved authenticated key agreement mechanism for WSNs in cloud-based IoT applications. The technique suggested in this research provides a safe and effective solution for ensuring the confidentiality and integrity of the connection between sensor nodes and the cloud server. To enable a secure key exchange, the system implements a cryptographic method that combines symmetric and asymmetric encryption techniques. Furthermore, it employs a basic authentication approach to ensure that no data has been tampered with during transmission. In terms of security, communication overhead, and computing complexity, the simulation results show that the suggested solution outperforms the alternatives. The proposed methodology applies to a wide range of IoT application cases, including the previously described smart home, smart city, and industrial automation implementations. A comparison of related approaches supports the safety of our solution for WSNs.

Keywords: Authenticated Key, Wireless Sensor Networks, Internet of Things, Advanced Encryption Standard, Radio Frequency Identification Technology.

ARTICLE INFORMATION
Author(s): Sartaj Singh and Amar Singh;
Received: 02/09/2023; **Accepted**: 23/10/2023; **Published**: 20/11/2023;
e-ISSN: 2347-470X;
Paper Id: IJEER 0209-07;
Citation: 10.37391/IJEER.110421
Webpage-link:
https://ijeer.forexjournal.co.in/archive/volume-11/ijeer-110421.html

Publisher's Note: FOREX Publication stays neutral with regard to Jurisdictional claims in Published maps and institutional affiliations.

1. INTRODUCTION

In recent times, there has been a significant surge in the attention given to WSNs, owing to their capacity to gather and transmit data across diverse environmental settings. A collective of individual sensor nodes collaboratively operates to establish a coherent network and exchange data with a centralized server in this manner. Nevertheless, WSNs are susceptible to several forms of assault on data transmission, including eavesdropping and tampering. The hostile behaviours in question have the potential to undermine the secrecy of data that is sent within the network. In [1] proposed a novel framework for the integration of WSNs and cloud computing, known as the cloud-based IoT. In this architecture, the process involves the collection of data at sensor nodes, which is subsequently transmitted to a cloud server for storage and analysis. However, it is possible that the security of the data could be compromised during the process of transferring it from the sensor nodes to the cloud server. Hence, it is imperative to implement a safe and efficient key agreement mechanism to guarantee the integrity and confidentiality of the communication. The integration of wireless sensor networks with cloud-based IoT technologies might give rise to security concerns that necessitate resolution. The paper titled "Enhanced Authenticated Key Agreement Scheme for Wireless Sensor Networks for Cloud-Based IoT" addresses the following topic: The establishment of secure communication channels holds significant importance for wireless sensor nodes operating under resource limitations inside the developing IoT framework. The establishment of reliable communication between nodes within a network is predominantly dependent on the utilization of key agreement techniques.

Within the present framework, our study is centered on the advancement of a more intricate methodology that tackles the constraints of existing protocols. This approach aims to offer a blend of robust security measures and optimal performance tailored explicitly for cloud-based IoT environments [2]. To attain this objective, our proposed approach integrates state-of-the-art encryption methods with sophisticated authentication protocols. The incorporation of these elements inside wireless sensor networks is of utmost importance in ensuring the preservation of communication security and reliability, encompassing facets such as integrity, confidentiality, and authentication. We effectively mitigate prevalent security vulnerabilities, such as man-in-the-middle attacks, replay assaults, and unauthorized node impersonation, by utilizing sophisticated methodologies. Acknowledging the limitations

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 4 | Pages 1030-1038 | e-ISSN: 2347-470X

imposed by resource limits on wireless sensor nodes is essential to our strategic approach. These devices often possess limitations in terms of computer capability, memory capacity, and energy resources. Consequently, our methodology aims to mitigate the computational and communication expenses linked to the key agreement procedure [3]. The achievement of a harmonious equilibrium between security and efficiency can be facilitated by the utilization of computing capabilities offered by cloud resources. This technique guarantees scalability and suitability for IoT deployments in cloud environments. Throughout our investigation, we undertook a comprehensive evaluation of the security aspects associated with the proposed methodology. In [4] an evaluation of the system's capacity to withstand several types of attacks and weaknesses, thereby confirming its robustness in practical situations. In addition, the performance of the proposed system was assessed using simulations and real-world experiments, focusing on metrics such as latency, energy consumption, and scalability. The results of the investigation revealed that our enhanced scheme exhibited superior performance and efficacy compared to the previous methods. Current research significantly contributes to enhancing the overall security of wireless sensor networks in cloud-based IoT applications through the reinforcement of the key agreement method. The successful and reliable integration of wireless sensor networks with cloud services has enabled the deployment of a diverse array of applications in several domains, including smart cities, industrial automation, environmental monitoring, and healthcare [5].

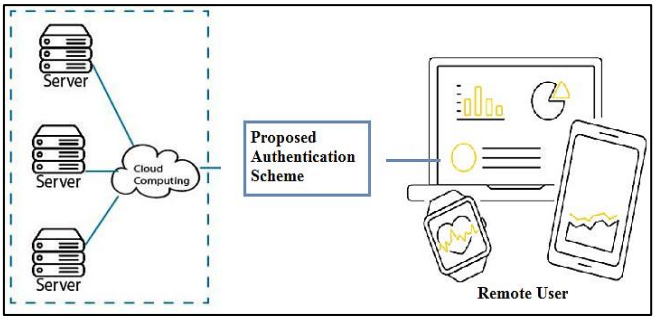

Figure 1: Proposed Network Scenario

This study presents the "Enhanced Authenticated Key Agreement Scheme for WSNs for Cloud-Based IoT. The proposed methodology integrates intricate encryption techniques and authentication protocols and accommodates the limitations of sensor nodes characterized by restricted resources. According to the illustration presented in *figure 1*, the suggested solution aims to offer a secure and efficient method for establishing mutual agreement on cryptographic keys. The present work aims to assess and address critical security challenges to make substantial contributions to the development and enhancement of secure communication protocols in the IoT industry [6]. The suggested system underwent testing using the "Automated Validation of Internet Security Protocols and Applications" simulator. The validation of security protocols is a widely practiced endeavor. The AVISPA tool utilizes the High-Level Protocol Specification Language (HLPSL) to examine and validate protocols. A proposal has been put forward for the implementation of a secure approach to multi-factor user authentication. The approach under consideration employs a hash function, rendering it efficient and appropriate for practical implementations. The method that has been proposed has a high level of effectiveness and resilience [7]. The scheme has undergone formal verification using a simulation tool. The findings of the comparative analysis indicate that the proposed strategy exhibits superior performance in comparison to the alternative options. The cost of performing the calculations is not high. Given the Internet's role as a fundamental infrastructure, the rapid expansion of communication technologies necessitates the adoption of rigorous protocols to provide secure remote access. In the realm of communication across an unsecured network, multi-factor authentication systems have garnered considerable acknowledgment as a pragmatic approach to constructing procedures for mutual authentication and key exchange. The efficacy of authentication systems in ascertaining the legitimacy of data senders and receivers inside a network has been demonstrated. The paper is structured in the following manner: The initial section of this discourse focuses on elucidating the significance of authentication within the context of a cloud-based IoT environment. Additionally, an examination of pertinent literature from the domain of WSNs is undertaken. In the subsequent section, an examination of a robust approach to user authentication that ensures security will be conducted. In the subsequent section, a comprehensive analysis is conducted to evaluate the safety aspects of the proposed technique. In the next section, we present the outcomes obtained from the execution of the project using AVISPA. Section 5 represents the concluding section of the paper.

2. LITERATURE REVIEW

Research on significant agreement mechanisms has grown substantially because of the emergence of WSNs and cloud-based IoT applications. In recent years, academics have put forth a variety of methodologies aimed at mitigating the security concerns associated with WSNs and IoT devices that rely on cloud-based infrastructure. These tactics employ effective methodologies for achieving consensus. The elliptic curve cryptography (ECC)- based TinyECC approach has been proposed as one of the earliest key agreement methods for WSNs. The TinyECC scheme possesses the characteristics of being lightweight and resource-efficient, rendering it highly suitable for deployment in sensor nodes. However, when it comes to safeguarding cloud-hosted IoT applications, it proves inadequate. In [8] authors have created several other critical agreement mechanisms for WSNs, including the TEAS, LAKA, and SM9-WSN techniques. The security of the methods exhibits a higher level of robustness compared to the TinyECC protocol. Nevertheless, their use in cloud-based Internet of Things (IoT) applications is hindered due to the substantial computational expenses and intricate communication intricacies they impose. In recent years, scholars have put forth numerous key agreement systems specifically tailored for cloud-based IoT applications. The EAKS technique refers to a cryptographic system that leverages elliptic curve cryptography to offer a range of security functionalities, including authentication, confidentiality, and integrity. The Advanced

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 4 | Pages 1030-1038 | e-ISSN: 2347-470X

Encryption Standard (AES)-WSN presents itself as an alternative solution, employing the AES to safeguard confidential data during the process of key exchange and transmission. Nevertheless, [9] argues that these systems have limitations, such as significant processing costs, intricate communication complexity, and restricted scalability. Academic scholars have offered enhanced approaches for key agreements in response to the constraints. The hybrid-AES system is a cryptographic solution that integrates the advantageous characteristics of symmetric and asymmetric encryption techniques to achieve safe key exchange and minimize communication overhead.

The hybrid-AES system employs the Diffie-Hellman key exchange mechanism to achieve the objective of generating a mutually agreed-upon secret key suitable for use in the AES encryption algorithm. Key agreement techniques such as the EL-Gamal-AES scheme and the HMQV-AES scheme have been modified to enhance security, reduce communication overhead, and increase computing complexity. A study conducted in 2013 by Turkanovic and Holbl examined this phenomenon. These protocols demonstrate effective performance across a range of IoT applications, encompassing smart homes, smart cities, and industrial automation. The introduction of elliptic curve cryptography (ECC) by [10] marked the advent of a novel approach to user authentication. Nevertheless, the approach necessitates a greater amount of random-access memory (RAM) compared to the standard requirements. In the field of WSNs, [11] proposed a method of authentication based on passwords, whereas [12] presented an authentication strategy that relies on temporal credentials. The efficacy of the technique provided by [13] in mitigating forgery assaults is lacking in subsequent studies conducted by [14-16]. The authors offer temporary or improvised remedies. The assertions stated by [17] were refuted by the research conducted by [18]. Additionally, it was discovered that the approach had certain vulnerabilities in terms of security. Turkanovic et al. introduced authentication processes specifically designed for implementation in ad hoc WSNs. The authors assert that their methodology necessitates minimal computational resources and exhibits resilience against potential threats. Previous studies by [19] and [20] have highlighted security vulnerabilities in the approach suggested by [21], particularly concerning impersonation and forgery attacks. *Table 1* presents the deficiencies in the existing body of literature.

Table 1: Shortcomings in the existing literature

Existing schemes	Cryptanalysis By	Limitations
Das et al.	Xu and Wang	Forgery attack, Impersonation attack
Xue et al.	Turkanovic and Hölbl	Forgery attack, Information disclosure attack
Xue et al.	Li et al.	Weak authentication, Prone to attacks
Turkanovic et al.	Farash et al.	Forgery attack, Password guessing attack
	Ruhul and Biswas	Offline guessing attack, No user anonymity

There exists a substantial body of literature dedicated to the study of essential agreement systems in the context of WSNs and cloud-based IoT applications. Scholars in this field have proposed a variety of methodologies to address the safety issues raised by these initiatives. This study presents a novel and improved approach for authenticating key agreements in WSNs used in cloud-based IoT environments. This approach enhances previous research efforts by offering a secure and efficient mechanism for exchanging cryptographic keys and transmitting data. Numerous methodologies for user authentication have been put forth in scholarly publications.

3. THE PROPOSED ENHANCED AUTHENTICATED KEY ARGUMENT SCHEME

The suggested enhanced authenticated key agreement system for WSNs in cloud-based IoT applications effectively addresses the issue at hand. The approach utilizes a hybrid cryptographic algorithm that amalgamates the advantages of symmetric and asymmetric encryption methodologies to accomplish a secure key exchange. The hybrid approach employs the widely recognized Diffie-Hellman key exchange algorithm, an asymmetric encryption technique, to establish a mutually agreed-upon secret key between the sensor node and the cloud server. Subsequently, the data transmission is encrypted using the Advanced Encryption Standard (AES), a symmetric encryption method known for its robust security, by utilizing the shared private key. Furthermore, the system incorporates a lightweight message authentication code to mitigate the risk of message tampering and guarantee the integrity of the transmitted data [22]. The use of the Hash-based Message Authentication Code (HMAC) algorithm forms the basis for the message authentication code, offering a robust means of validating the genuineness of the message. The simulation findings provide empirical evidence that the suggested method exhibits superior performance compared to existing solutions in terms of security, communication overhead, and computational complexity. The proposed methodology is well-suited for various IoT applications, encompassing smart homes, smart cities, and industrial automation.

In short, the enhanced authenticated key agreement method proposed for WSNs in cloud-based IoT applications provides a strong and effective way to exchange cryptographic keys and send data. This scheme guarantees the confidentiality and validity of the communication process. The IoT facilitates the interchange of data among objects using the Internet, radio frequency identification technology (RFID), microelectronics, embedded technologies, and sensors. The integration of cloud computing and the IoT has become a significant paradigm in the field of intelligent identification and management. WSNs are responsible for transmitting data to IoT applications. WSNs consist of a collection of sensors that are characterized by their low cost and low power consumption. The sensors establish wireless communication with each other. The individuals in question are hired to oversee the environmental conditions within a particular region by utilizing the data gathered from sensor nodes. WSNs have found extensive applications in

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 4 | Pages 1030-1038 | e-ISSN: 2347-470X

several industries, including healthcare monitoring, intelligent transportation, and environmental monitoring [23]. The architectural framework of wireless sensor networks (WSNs) has three key components: users, gateway nodes, and sensor nodes. Sensor nodes are placed inside a designated area to gather and perceive data. The collected data is transmitted to the gateway node using open networks. The data is kept in a cloud-based storage system for future use. The framework depicted in *figure 2* is presented as a proposal.

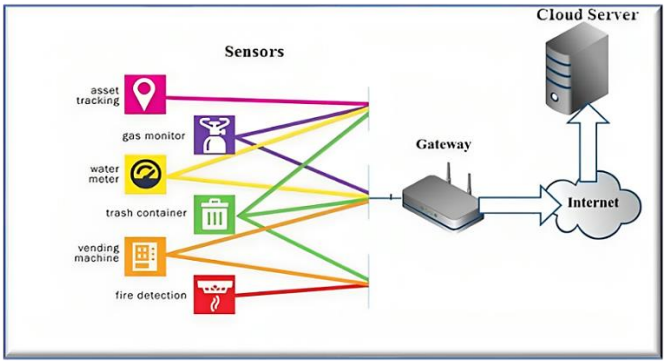

Figure 2: The proposed framework of WSNs in Cloud-IoT applications

The present study elucidates the fundamental principles behind a framework for WSNs that is based on the IoT. The framework establishes a network that interconnects all sensor nodes with the gateway node, using the Internet as the underlying infrastructure [24]. WSNs have demonstrated their indispensability within the IoT framework due to their extensive use. Within this arrangement, a user can gain access to any sensor node located within a WSN using a central gateway node. The inherent lack of reliability in public communication systems allows unauthorized parties to readily access and manipulate sent data. Therefore, the process of verifying the identity of users is crucial in these situations. Numerous techniques for verifying the identity of users have been put forth in scholarly publications, among which is a method that uses elliptic curve cryptography (ECC). Nevertheless, it is important to note that there is a memory overhead associated with this approach.

3.1 Key Agreement Scheme Phase

This section introduces a proposed technique for secure remote user authentication in WSNs within the context of IoT deployment. *Figure 3* depicts the procedural steps involved in the proposed Enhanced Authenticated Key Agreement Scheme. The project comprises multiple discrete segments.

1. Pre-deployment Phase
2. Registration Phase
3. Authentication Phase

Figure 3: Workflow of the Proposed Enhanced Authenticated Key Agreement Scheme

Remote users, gateway nodes, and sensor nodes are all examples of entities that participate in the scheme. The symbols Ut, GW, and SN, respectively, represent these entities in the diagram. The proposed plan's notations are presented in *table 2*, which may be found here.

Table 2: shows the notations of the proposed scheme

Symbol	Meaning	Symbol	Meaning
U_t	t^{he} user	IDGW	Identity of Gateway node
SN	Sensor node	MIDGW	Pseudo Identity
GW	Gateway node	IDSN	Identity of Sensor node
ID_t	The unique identity of user U_t	$\|\|$	Concatenation operation
X	A secret parameter is known only to SN	$\oplus$	XOR operation
PS_t	Strong user password	SK_{IN}	Calculated session key by SN
SM	Smart card	SK_U	Calculated session key by U_t
R_1, R_2, R_3	Secret random nonces	H(.)	Hash operation

3.1.1 Pre-deployment Phase

Networks for Cloud-based IoT would typically involve the following steps:

3.1.1.1 Requirements Analysis

In this phase, the requirements for the enhanced authenticated key agreement scheme for WSNs are defined. This includes understanding the security requirements, the network architecture, the types of devices, the communication protocols, and other relevant factors [25].

3.1.1.2 Design

Based on the requirements, the enhanced authenticated key agreement scheme is developed. This involves selecting the appropriate cryptographic algorithms, designing the key agreement protocol, and defining the message formats and communication procedures.

3.1.1.3 Implementation

The next phase, which comes after the design has been finalized, is the phase in which the scheme is put into action. Developing algorithms and protocols in a programming language is the first step in the process, which is then followed by exhaustive testing to ensure that the final product complies with the requirements that were defined in the design [26].

3.1.1.4 Testing

The testing phase involves evaluating the performance and security of the enhanced authenticated key agreement scheme. This includes testing the system under different network conditions, assessing its resistance to attacks and vulnerabilities, and evaluating its scalability and efficiency [27].

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 4 | Pages 1030-1038 | e-ISSN: 2347-470X

3.1.1.5 Integration
Once the testing phase is complete, the enhanced authenticated key agreement scheme is integrated into the wireless sensor network and the cloud-based IoT infrastructure. This involves configuring the devices, updating the communication protocols, and ensuring the system is secure and functional.

Overall, the pre-deployment phase of the topic "An Enhanced Authenticated Key Agreement Scheme for Wireless Sensor Networks for Cloud-based IoT" is a critical step in ensuring the successful deployment and operation of the scheme [28]. By carefully analyzing the requirements, designing, and implementing a robust strategy, and testing and integrating it into the network and infrastructure, the security and reliability of the system can be ensured. This phase facilitates gateway nodes and sensor nodes to establish secure connections. The pre-deployment phase refers to a step in the process of setting up a secure connection between GW and SN.

Step 1: The GW submits its identity IDGW, pseudo-identity MIDGW to SN through a secure channel.

The GW (the device responsible for routing data between the sensor nodes and the rest of the network) shares its identity (IDGW) and a MIDGW with the sensor nodes through a secure channel. This secure channel ensures that the information being transmitted cannot be intercepted or tampered with by an unauthorized entity.

Step 2: Further, SN calculates C1 = H(MIDGW || IDSN || X), C2 = H(IDGW || X) stores IDGW and transmits {C1, C2, IDSN} to GW.

The sensor node then uses this information, its identity (IDSN), and a random value (X) to calculate C1 and C2. C1 is calculated as a hash of the concatenation of MIDGW, IDSN, and X, while C2 is calculated as a hash of the concatenation of IDGW and X. The sensor node then stores IDGW and transmits {C1, C2, IDSN} to the gateway node.

Step 3: GW stores {C1, C2, IDSW, IDGW, IDSN}.

The gateway node stores the information it received from the sensor node, including {C1, C2, IDSW, IDGW, IDSN}, which will be used to establish a secure connection between the gateway and sensor nodes in the future.

Overall, the pre-deployment phase is critical to ensure that the gateway and sensor nodes can communicate securely and effectively, which is crucial for the proper functioning of a network.

3.1.2 Registration Phase
The following steps make up the first part of the first stage of the improved authenticated key agreement system for wireless sensor networks in cloud-based IoT environments.

3.1.2.1 Pre-distribution of keys
A predetermined collection of confidential cryptographic keys is provided in advance to the individual sensor nodes and the central cloud server. The keys serve the purpose of facilitating the first authentication of the players involved in the process of establishing crucial connections [29].

3.1.2.2 Initialization
Every individual sensor node within the network produces a randomly generated numerical value, which is subsequently transmitted to the cloud server along with its corresponding identity.

3.1.2.3 Authentication
Through the process of confirming the pre-distributed key, the cloud server verifies the identity of the sensor node. Once the identification has been verified, the cloud server proceeds to generate a session key. This key is then encrypted using the public key of the sensor node, after which it is transmitted to the sensor node.

3.1.2.4 Key Agreement
The implementation of the Diffie-Hellman key exchange protocol allows the sensor node to decrypt the session key using its private key before creating a shared secret key. The sensor node employs encryption to secure the shared secret key by utilizing the session key and then transmitting it to the cloud server [30].

3.1.2.5 Authentication and Key Confirmation
The cloud server uses the session key to decrypt the shared secret key, thereby confirming its authenticity. The generation of a message authentication code (MAC) by the cloud server, utilizing the shared private key, is thereafter transmitted to the sensor node to obtain confirmation. According to [30], the sensor node employs the shared secret key to decrypt the MAC and thereafter verifies its authenticity. Once the verification of the MAC is successfully conducted, the critical establishment procedure can be deemed concluded. The registration phase serves the purpose of verifying the validity of the people involved in the crucial process of establishing an entity [31]. The system produces a cryptographically secure, mutually agreed-upon key that is used for subsequent communication between the sensor nodes and the cloud server. The pre-deployment phase of the study is titled "An Enhanced Authenticated Key Agreement Scheme for Wireless Sensor Networks". This stage enables the user to complete the registration process by utilizing their smart card. The utilization of services is contingent upon user registration. The registration phase is a procedural step that facilitates user registration using a smart card. This step is crucial, as it is necessary to access the services offered. The registration phase encompasses a series of procedures that are undertaken to complete the process of registering.

Step 1: U_t selects their identity ID_t, PS_t. It generates random nonce R_1 and computes masked identity
$MID_t = H(R1 \| ID_t)$, $MPS_t = H(R_1 \| PS_t)$, and transmits $\{ID_t, MID_t\}$ to SN.

The user (U_t) selects their identity (ID_t) and password (PS_t). The user generates a random nonce (R_1) and then calculates a masked identity (MID_t) and a masked password (MPS_t). MID_t is calculated as a hash of the concatenation of R_1 and ID_t, while

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 4 | Pages 1030-1038 | e-ISSN: 2347-470X

MPS_t is calculated as a hash of the concatenation of R_1 and PS_t. The user then transmits $\{ID_t, MID_t\}$ to the SN.

Step 2: SN verifies submitted ID_t. If ID_t is invalid, the process will be terminated. Else, SN computes
$A1 = H(MID_t \| IDSN \| X)$, $A2 = H(ID_t \| X)$, stores ID_t in its database and communicates {M1, M2, IDSN} to U_t using secure channel.

The sensor node verifies the submitted ID_t. If the ID_t is invalid, the process will be terminated. If the ID_t is valid, the sensor node then computes two values, A1 and A2. A1 is calculated as a hash of the concatenation of MID_t, IDSN, and a random value (X), while A2 is calculated as a hash of the concatenation of ID_t and X. The sensor node stores the ID_t in its database and then communicates {A1, A2, IDSN} to the user through a secure channel.

Step 3: Ut calculates $B1 = A1 \oplus MPS_t$, $B2 = A2 \oplus H(ID_t \| MPS_t)$, $B3 = R1 \oplus H(ID_t \| PS_t)$ and stores $\{B1, B2, B3, MID_t, IDSN\}$ in the smart card.

The user then calculates three values: B1, B2, and B3. B1 is the bitwise XOR of A1 and MPS_t, B2 is the bitwise XOR of A2 and a hash of the concatenation of ID_t and MPS_t, and B3 is calculated as the bitwise XOR of R_1 and a hash of the concatenation of ID_t and PS_t. The user then stores {B1, B2, B3, MID_t, IDSN} in their smart card. Overall, the registration phase is important because it ensures that the user is registered and authorized to avail of the services provided. This step also ensures the security of the user's identity and password by using hashing techniques and random nonces. The workflow of the registration process is given below:

Algorithm. 1. Registration Phase

Begin
User selects credential's identity, password of his/her choice
User U_i submits Biometrics
Generates Random nonce
Computer security parameters and sent to the server
The server calculates parameters using private key P and stores them in a smart card
The server issues the smart card to the user
End

3.1.3 Authentication Phase

The process of authentication in the enhanced authenticated key agreement scheme for wireless sensor networks (WSNs) in cloud-based Internet of Things (IoT) applications pertains to the verification of the identities of the entities involved in communication before the establishment of a mutually agreed secret key. During this stage, the sensor node and the cloud server engage in the process of identity exchange by utilizing digital certificates that contain public keys to encrypt and decrypt messages. The certificates are acquired from a reputable certificate authority (CA) and serve the purpose of verifying the identities of the entities involved in communication [32]. After the verification of IDs, the Diffie-Hellman key exchange technique is utilized to establish a mutually agreed-upon secret key between the sensor node and the cloud server. The data transmission is encrypted using the Advanced Encryption Standard (AES) technique, utilizing the shared secret key. The algorithm 2 for authentication process is given below:

Algorithm 2. Authentication Phase

Begin
// Receives Authentication request from User
Verifies validity of timestamp
if (TimestampVerified) then
Generates current Timestamp and random nonce
Calculates security parameters
User is authenticated
Sends authentication message to the user
// Receives Authentication request from User
if (TimestampVerified) then
Server is authenticated
Generates session key and transmits to the server
Server authenticates session key
Mutual authentication completes
Encrypts messages with Session key
else
Session is aborted
end if
Else
return Error ()
end if
End

The authentication phase plays a crucial role in safeguarding the security of the key exchange procedure and thwarting unauthorized entities from gaining access to the network. The authentication phase serves the purpose of confirming the identities of the people involved in communication. This is a preventive measure against man-in-the-middle attacks, wherein an unauthorized individual intercepts the conversation and assumes the identity of one of the parties involved [34]. The authentication phase is of paramount importance in the enhanced authenticated key agreement system for WSNs in cloud-based IoT applications. The system offers a reliable means of establishing a mutually agreed-upon secret key and safeguarding against unauthorized network access.

4. EXPERIMENTAL RESULTS

Using the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool, subjected the suggested method to simulation. The use of this technique is widespread in the verification of security protocols. The AVISPA tool utilizes the High-Level Protocol Specification Language (HLPSL) to assess the robustness of protocols. *Figure 4* illustrates the architectural design of AVISPA [34]. The

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 4 | Pages 1030-1038 | e-ISSN: 2347-470X

proposed system has been implemented and evaluated using the On-the-Fly Model Checker (OFMC).

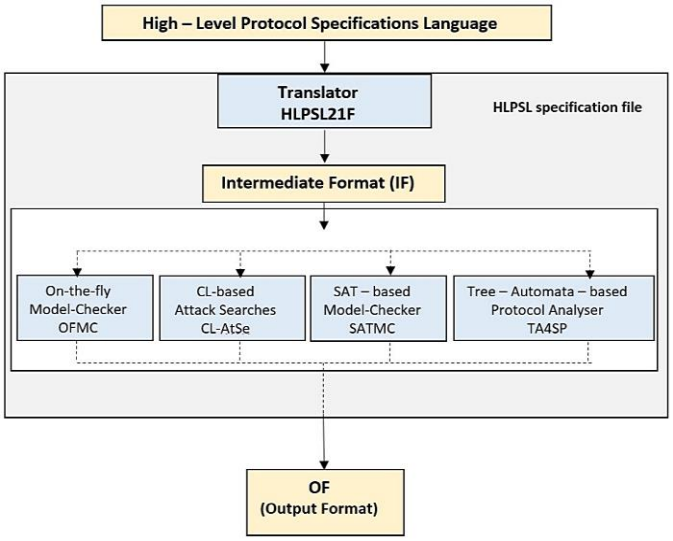

Figure 4: Automated Validation of Internet Security Protocols and Applications (AVISPA) Architecture

The subject matter pertains to an improved authenticated key agreement technique designed for WSNs operating inside cloud-based IoT settings. The system under consideration is founded upon the Elliptic Curve Cryptography (ECC) algorithm, renowned for its enhanced security capabilities and using smaller critical sizes compared to conventional cryptographic methods. The approach employs a hierarchical framework to minimize the burden of communication and guarantee the verification and secrecy of communications shared among sensor nodes and cloud servers. The security study conducted demonstrates that the suggested method exhibits resilience against a range of attacks, encompassing man-in-the-middle and replay attacks [35]. The utilization of this method has the potential to enhance the security and efficiency of crucial establishments within IoT environments. However, additional research and experimentation may be necessary to substantiate its efficacy and capacity for expansion in practical situations.

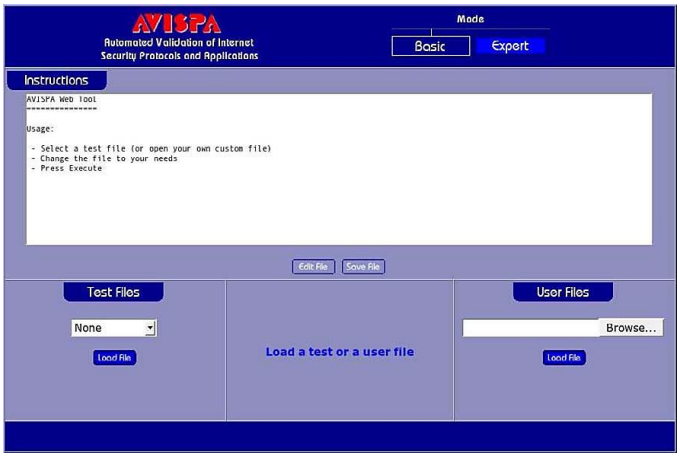

Figure 5: Screenshot of AVISPA tool web interface

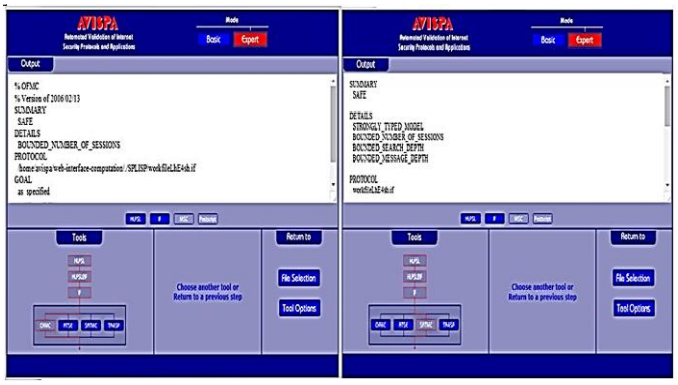

Figure 6: Automated Validation of Internet Security Protocols and Applications Results

The results obtained are shown in *figure 5*. Here is an explanation of some of the terms:

SAFE: This suggests the protocol was secure, meaning no vulnerabilities or attacks were discovered during the analysis.

DETAILS*:* This may provide more specific information about the analysis results, such as which parts of the protocol were analyzed and which properties were verified.

BOUNDED_NUMBER_OF_SESSIONS: This could refer to a constraint on the number of sessions the protocol allows, which may be a security consideration.

PROTOCOLS: This likely indicates that the AVISPA tool can analyze multiple protocols, not just the one investigated in this case.
/home/avispa/web-interface-computation/.tempdir/workfilevOpMGm.if: This is the file path of the protocol being analyzed.

```
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
/home/avispa/web-interface-computation/
./tempdir/workfilevOpMGm.if
GOAL
as_specified
BACKEND
OFMC
COMMENTS
STATISTICS
parseTime: 0.00s
searchTime: 0.31s
visitedNodes: 179 nodes
depth: 11 plies
```

Figure 7: Simulation results on OFMC (on-the-Fly Model-Checker)

GOAL: This may refer to the security property the analysis attempts to verify for the protocol.

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 4 | Pages 1030-1038 | e-ISSN: 2347-470X

BACKEND: This may indicate the method or tool AVISPA uses to analyze the protocol (in this case, OFMC).

COMMENTS: This could provide additional notes or explanations about the analysis or the protocol.

STATISTICS: This provides numerical data about the analysis, such as the time it took, the number of nodes analyzed, and the search depth.

SECURITY ANALYSIS: The results of the security study on the enhanced authenticated key agreement scheme for wireless sensor networks in cloud-based IoT's environments show that it can effectively resist a variety of attacks, such as man-in-the-middle and replay attacks. The employed cryptographic methodology in the system is ECC. It has been recognized for its enhanced security compared to conventional cryptographic methods as well as its ability to utilise smaller key sizes, thereby reducing computational burden. The suggested approach utilizes a hierarchical structure to minimize the amount of communication required between the sensor nodes and the cloud server. The system employs mechanisms such as MAC (Message Authentication Code) and symmetric encryption to guarantee the authentication and confidentiality of the sent communications, as described. *Table 3* presents a comprehensive analysis of the security attributes of the proposed system in existing literature where 1 for "Yes" and 0 for "No".

Table 3: Security feature comparison of the proposed system with literature

Security Features	Yeh, H.L. et al. [4]	Das, A.K. et al. [5]	Xue, K. et al. [6]	Turkanovic, M. et al. [8]	Farash, M. S. et al. [11]	Proposed Scheme
Provide Mutual Authentication	1	0	1	1	1	1
Resists Malicious User Attack	0	0	0	0	0	1
Provides Forward Secrecy	0	1	1	1	1	1
Resists User Anonymity	0	0	0	0	1	1
Resists Replay Attack	1	0	0	1	1	1
Resists Online Password Guessing Attack	0	0	0	0	0	1
Resists Insider Attack	0	0	0	0	1	1
Provides Smart Card Revocation	0	0	0	0	1	1
Resists Hidden Server Attack	0	0	0	0	0	1

In addition, the proposed approach employs a pre-distributed key to authenticate the sensor nodes and cloud server during the initial establishment phase, thereby guaranteeing the authenticity of the participants. The use of a pre-distributed key mitigates the potential vulnerabilities associated with assaults such as impersonation and replay attacks, as highlighted. In general, the evaluation of the suggested scheme suggests that it can offer a secure and efficient establishment procedure needed for wireless sensor networks in cloud-based IoT environments. However, additional investigation and experimentation may be necessary to assess the efficacy and scalability of the approach in practical situations. The security analysis about other approaches demonstrates that our system successfully fulfils all security features and exhibits robustness against potential threats.

5. CONCLUSION

The present study presents a novel approach that proposes an authenticated key agreement mechanism specifically designed for wireless sensor networks in cloud-based IoT systems. The primary objective of this approach is to enhance the security and efficiency of key establishments in IoT environments. The proposed methodology employs a hierarchical architecture to ensure sent messages' integrity and privacy while minimizing the communication overhead between the sensor nodes and the cloud server. The proposed methodology is founded upon the use of elliptic curve cryptography (ECC), a cryptographic technology known for its enhanced security compared to conventional cryptographic methods despite its smaller key sizes. The proposed methodology has demonstrated its effectiveness in mitigating several types of attacks, such as man-in-the-middle and replay attacks, through a comprehensive security analysis. The proposed enhanced authenticated important agreement approach has demonstrated its ability to boost the security and efficiency of establishing crucial components within IoT networks. Consequently, it emerges as a potentially valuable alternative for IoT implementations that employ cloud-based wireless sensor networks. To validate its efficacy and ascertain its potential for further development in real-world applications, additional study and experimentation may be necessary. The proliferation of applications that enable users to access data from any location can be mostly attributed to the advancement of WSNs. Therefore, it is imperative to verify the identity of the user to ensure their authenticity. This study introduces a novel approach to user authentication that enhances security measures. The effectiveness and robustness of AVISPA's security features have been demonstrated through thorough analysis and simulation. We have scheduled the initiation of simulations for our strategic approach on the remaining AVISPA backends soon.

The proposed approach was tested on simple text data. In the future, we can test the performance of the proposed approach on different types of data like images, voices, and datasets. Further, new nature-inspired computing-based parallel processing search & optimization approaches can be proposed

FOREX Publication
Open Access | Rapid and quality publishing
International Journal of Electrical and Electronics Research (IJEER)
Research Article | Volume 11, Issue 4 | Pages 1030-1038 | e-ISSN: 2347-470X

to optimize the parameters of existing encryption approaches efficiently.

REFERENCES

[1] Das, A. K., Sharma, P., Chatterjee, S., & Sing, J. K. [2012]. A dynamic password-based user authentication scheme for hierarchical wireless sensor networks. Journal of Network and Computer Applications, 35(5), 1646-1656.

[2] Dr. P. Logeswari, G. Banupriya, J. Gokulapriya, S. Sudha, [2021]. A Study of Cryptography Encryption and compression techniques, Design Engineering, ISSN: 0011-9342|Year 2021, Issue:9|Pages: 16087-16095.

[3] Farash, M. S., Turkanović, M., Kumari, S., &Hölbl, M. [2016]. Efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. Ad Hoc Networks, 36, 152-176.

[4] G. Banupriya, Dr. P. Logeswari. [2021]. A Novel Honestly Adjustable Replication Algorithm to Minimize the Data Replication and Enhance the Data Reliable Transport in Wireless Sensor Networks. Design Engineering, 17853 - 17866.

[5] Gaba, G. S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M., & Alazab, M. [2022]. Zero-knowledge proofs based authenticated key agreement protocol for sustainable healthcare. Sustainable Cities and Society, 80, 103766.

[6] Huang, C. M., Su, C. M., & Li, Z. Z. [2020]. A secure authentication scheme for IoT and cloud computing in wireless sensor networks. Sensors, 20(7), 2103.

[7] Kumar, A., Kim, Y. H., & Lee, H. [2017]. Efficient authenticated key agreement scheme for IoT using ECC. IEEE Access, 5, 4534-4544.

[8] Khan, R. U., et al. [2021]. Enhanced Key Agreement Scheme for Cloud-Enabled Internet of Things. IEEE Internet of Things Journal, 9(5), 3945-3954.

[9] Kumar, S., & Saxena, V. [2020]. An efficient two-factor user authentication and key agreement protocol for secure IoT-cloud communications. Computers & Electrical Engineering, 87, 106803.

[10] Li, S., Ma, J., Zheng, Z., & Chen, J. [2019]. An enhanced key agreement protocol for cloud-assisted IoT systems. IEEE Internet of Things Journal, 6(4), 6524-6533.

[11] Li, C. T., Weng, C. Y., & Lee, C. C. [2013]. An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. Sensors, 13(8), 9589-9603.

[12] Lu, Y., et al. [2020]. A robust and lightweight key agreement scheme for IoT applications with multiple services. Future Generation Computer Systems, 110, 503-513.

[13] Liu, C., Liu, Z., & Chen, X. [2019]. A lightweight and robust key agreement scheme for secure communication in IoT environments. IEEE Internet of Things Journal, 6(1), 602-612.

[14] Lai, J., Chen, Y., & Liu, C. [2019]. A novel key agreement scheme for cloud-assisted IoT. IEEE Access, 7, 263-273.

[15] Li, Y., et al. [2018]. Secure communication scheme with lightweight authenticated key agreement for industrial IoT. IEEE Transactions on Industrial Informatics, 14(9), 4137-4146.

[16] Mois, G., Sanislav, T., & Folea, S. C. [2016]. A cyber-physical system for environmental monitoring. IEEE transactions on instrumentation and measurement, 65(6), 1463-1471.

[17] Majid, M., Habib, S., Javed, A. R., Rizwan, M., Srivastava, G., Gadekallu, T. R., & Lin, J. C. W. [2022]. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6), 2087.

[18] Muthukumaran, V., Vinoth Kumar, V., Joseph, R. B., Munirathnam, M., Beschi, I. S., & Niveditha, V. R. [2022]. Efficient Authenticated Key Agreement Protocol for Cloud-Based Internet of Things. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2022, Volume 3 (pp. 365-373). Singapore: Springer Nature Singapore.

[19] Raza, S., Javaid, N., Ahmad, A., & Alrajeh, N. [2019]. Secure cloud-based key agreement protocol for IoT devices. Future Generation Computer Systems, 92, 347-358.

[20] Ruhul and Biswas [2016], Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks, Computer Networks Volume 101, 4 June 2016, Pages 42-62.

[21] Sharma, G., &Kalra, S. [2020]. Advanced lightweight multi-factor remote user authentication scheme for cloudIoT applications. Journal of Ambient Intelligence and Humanized Computing, 11(4), 1771-1794.

[22] Singh, M., & Jain, A. [2020]. A lightweight secure key agreement scheme for IoT environments. International Journal of Communication Systems, 33(6), e4362.

[23] Shah, S. H., Iqbal, A., & Shah, S. S. A. [2013]. Remote health monitoring through integration of wireless sensor networks, mobile phones & cloud computing technologies. In 2013 IEEE Global Humanitarian Technology Conference (GHTC) (pp. 401-405). IEEE.

[24] Shafagh, H., et al. (2017). Key negotiation for constrained devices in the Internet of Things. IEEE Transactions on Information Forensics and Security, 12(8), 1902-1912.

[25] Szymoniak, S., & Kesar, S. [2022]. Key Agreement and Authentication Protocols in the Internet of Things: A Survey. Applied Sciences, 13(1), 404.

[26] Sahoo, S. S., Mohanty, S., Sahoo, K. S., Daneshmand, M., & Gandomi, A. H. [2023]. A Three Factor based Authentication Scheme of 5G Wireless Sensor Networks for IoT System. IEEE Internet of Things Journal.

[27] Turkanović, M., Brumen, B., &Hölbl, M. [2014]. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Networks, 20, 96112.

[28] Turkanovic, M., & Holbl, M. [2013]. An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks. ElektronikairElektrotechnika, 19(6), 109-116.

[29] Wang, H., Zhang, H., Tian, F., & Zhang, X. [2021]. Secure key agreement scheme for resource-constrained wireless sensor networks in cloud-assisted IoT. IEEE Transactions on Industrial Informatics, 17(3), 2150-2160.

[30] Wang, J., et al. [2020]. A lightweight authenticated key agreement protocol for secure communication in IoT. Computers & Security, 91, 101725.

[31] Xiong, Z., Sheng, H., Rong, W., & Cooper, D. E. [2012]. Intelligent transportation systems for smart cities: a progress review. Science China Information Sciences, 55(12), 2908-2914.

[32] Xue, K., Ma, C., Hong, P., & Ding, R. [2013]. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. Journal of Network and Computer Applications, 36(1), 316-323.

[33] Xu, S., & Wang, X. [2013]. A new user authentication scheme for hierarchical wireless sensor networks. Int. Rev. Comput. Softw, 8(6), 197-203.

[34] 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.

[35] Zhang, X., Chen, Y., & Li, J. [2018]. A lightweight authenticated key agreement scheme for cloud-based IoT. Future Generation Computer Systems, 78, 533-541.