Journal of Theoretical and Applied Information Technology
15th December 2022. Vol.100. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURE AUTHENTICATION SCHEME BASED ON NUMERICAL SERIES CRYPTOGRAPHY FOR INTERNET OF THINGS

MAHA ALADDIN[1], KHALED NAGATY[2], ABEER HAMDY[3]

[1] British University in Egypt, Department of Software Engineering, ICS, Egypt

[2] British University in Egypt, Department of Computer Science, ICS, Egypt

[3] British University in Egypt, Department of Software Engineering, ICS, Egypt

E-mail: [1]maha.aladdin@bue.edu.eg, [2]khaled.nagaty@bue.edu.eg, [3]abeer.hamdy@bue.edu.eg

ABSTRACT

The rapid advancement of cellular networks and wireless networks has laid a solid basis for the Internet of Things. IoT has evolved into a unique standard that allows diverse physical devices to collaborate with one another. A service provider gives a variety of services that may be accessed via smart apps anywhere, at any time, and from any location over the Internet. Because of the public environment of mobile communication and the Internet, these services are highly vulnerable to a several malicious attacks, such as unauthorized disclosure by hostile attackers. As a result, the best option for overcoming these vulnerabilities is a strong authentication method. In this paper, a lightweight authentication scheme that is based on numerical series cryptography is proposed for the IoT environments. It allows mutual authentication between IoT devices. Parametric study and formal proofs are utilized to illustrate that the proposed approach is resistant to a variety of security threats.

Keywords: *Internet of Things, Confidentiality, Authentication, Cryptography, Security Scheme, BAN Logic*

1. INTRODUCTION

The Internet of Things is a new paradigm that has been hailed as a century-defining technology. It enables everyday things to interact with one another and provide services without the need for human involvement [1]. The Internet of Things' ultimate purpose is to eventually change human life throughout its intelligence and intellect. Because they are widely employed in IoT applications like environmental monitoring, disaster management, battlefield surveillance, industrial, healthcare, and assisted living, wireless sensor networks (WSNs) are one of the IoT's supporting technologies [2-6]. The sensed data, on the other hand, can be extremely sensitive and be intercepted by an unauthorized party [7, 8].

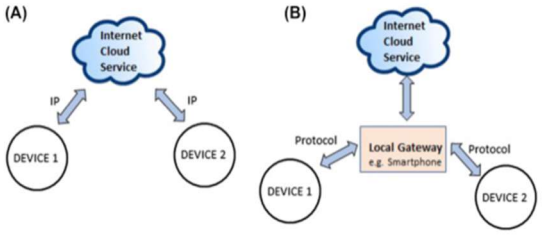

Figure 1: (A) Device-To-Cloud And (B) Device-To-Gateway Communication Models To Connect And Communicate Between A Number Of Devices.

Our lives are now more convenient thanks to the IoT. But in addition to offering us ease, the IoT also poses serious unrecognized risks. For instance, Amazon's Ring home security camera contains a security flaw that has been exploited. Hackers have uploaded a sizable number of videos and images of users online. Another illustration is malware called Silex, which has the ability to attack thousands of IoT devices, render them inoperable across a wide region, and result in significant losses in terms of people, property, and money. IoT security must be increased as a result to stop any further harm to human life. To address the aforementioned security issues, researchers have created a variety of solutions. The main approach entails encrypting all

communications and data sent over open channels. This would guarantee that during the communication phase, no information relating to any organization would be compromised. As a result, an authentication and key agreement (AKA) mechanism that is secure and effective is needed.

A secret key should be provided between communication parties to encrypt the transferred data to protect data transmission over a public channel. However, before negotiating the cryptographic key, it is critical to confirm the parties' identities. To ensure that only authorized organizations can access the provided information, mutual authentication and session key agreement are required [9, 10].

In this paper, we present an improved Numerical Series based technique for WSN authentication and session key agreement in the context of the Internet of Things. Because it delivers high-level security with a small key size, the Numerical Series Technique is more secure and ideal for limited situations [11]. The Burrows-Abadi-Needham (BAN) logic is used to formally verify the upgraded scheme's security. A comparison of our proposed technique to recent related methods [11-26] is also provided to demonstrate that it is safe and efficient.

2. RELATED WORK

Several authentication algorithms for IoT environments are examined by El-hajj et al. [7], Das et al. [8], and Ferrag et al. [9.] These protocols were created utilizing a variety of cryptographic techniques, including digital signatures, identity-based cryptography, physical unclonable functions (PUFs), symmetric and asymmetric cryptography. Two PUF-based IoT infrastructure authentication techniques were presented by Aman et al. [10]. Both protocols, on the other hand, are incapable of meeting security criteria.

Lamport [27] was the first to suggest using a username and password for authentication. In order to encrypt the password, a secure one-way function was used. This protocol, however, is reliant on an encrypted password table that is vulnerable to a stolen-verifier attack. Following that, numerous username-and-password-based authentication methods have been proposed. A multiserver authentication method based on neural networks was proposed by Li et al. [28]; however, Lin et al. demonstrated how difficult the protocol was. Furthermore, Cao et al. [29] discovered that the Li et al. authors proposed proto-col is susceptible to impersonation attacks and requires a lot of storage. Juang [30] pioneered the multiserver authentication system by introducing the use of a nonce and password. The proposed method in Juang was then shown by Ku et al. [31] to be insecure against insider assaults.

A hash function was utilized by Liao et al. [32] in the key management protocol in the multiserver scenario. After showing that the authentication method used by Liao et al. is not safe against a number of flaws, Hsiang et al. [33] upgraded the protocol. All of the currently used authentication protocols have security flaws, and a major issue with the majority of them is their great complexity. Amin et al [34] expanded authentication strategy for geo-distributed cloud systems uses IoT devices. They examined the protocol in Xue et al. [35] and found that it was not resistant to user impersonation and session key discloser attacks, nor was it given some of the security requirements, such as user anonymity. In order to store and retrieve all confidential information from private cloud servers, they consequently proposed a framework based on the geo-distributed cloud system. Additionally, they used the BAN logic model and the AVISPA program to validate their suggested authentication technique. Its defense against security threats such user impersonation, offline password guessing, session key discloser, privileged insider, and replay attacks was demonstrated. The primary flaw of Amin et al.'s protocol is that a hostile cloud server can impersonate the cloud server selected by a user, and the control server cannot detect this impersonation.

A key agreement protocol for IoT devices was presented by Gope and Sikadar [11]. Their protocol, on the other hand, is prone to desynchronization attacks and inefficient in terms of providing perfect forward secrecy. Based on self-generated MAC storage and the Merkle tree signature technique [13], Lyu et al. [12] suggested a key agreement and authentication system. However, their protocol [13] contains several security flaws. Salmdamli et al. [14] investigated the performance of the Merkle tree protocol on a variety of IoT devices in 2018.

Sun et al. [15] presented a key-agreement authentication scheme based on the hash function and the Advanced Encryption Standard (AES), but their protocol is not safe. Jan et al. [16] proposed a payload-based key agreement and privacy-preserving protocol for iOS infrastructure utilizing AES. For smart appliances, Song et al. [17] designed an upgraded authentication protocol. For data transfer, they used Message Authentication Codes (MAC).

There are various asymmetric cryptographic-based protocols that use Elliptic Curve Cryptography (ECC) [18] – [24]. ECC is compatible with devices

that have limited resources, such as IoT devices. An ECC-based key agreement and authentication technique for IoT environments was described by Kalra and Sood [21]. They claim [21] that their protocol has basic security measures. However, Chang et al. [19] examined Kalra and Sood's protocol and found that it does not support mutual authentication or session key agreement. Furthermore, Chang et al. [19] suggested an updated protocol to address the security weaknesses in Kalra and Sood's protocol [21].

Kumari et al. [25] investigated at the Kalra and Sood [21] protocol and discovered that it does not accomplish device anonymity, mutual authentication, or session key agreement. It is also subject to both insider and offline password guessing attacks. Kumari et al. [25] suggested an improved ECC-based key agreement protocol following that. Maarof et al. [22] cryptanalyzed the procedure subsequently.

Chikouche et al. [26] have introduced a privacy-preserving code-based authentication mechanism for the Internet of Things. We cryptanalyzed Chikouche et al protocols and observed that it is susceptible to an anonymity violation attack. Additionally, the protocol proposed by Chikouche et al. is vulnerable to device impersonation and session-specific data leaking attacks.

Even though a number of authentication and key agreement techniques have been developed, the majority of them are highly attackable and may also be ineffective in contexts with limited resources. The above-discussed protocols' weaknesses and vulnerabilities urge us to develop a new protocol that can overcome all of these security constraints. Designing an authentication mechanism that can enable safe communication between resource-constrained IoT components has therefore become essential. Therefore, we suggest in this research a lightweight and safe authentication key agreement technique for the Internet of Things based on a novel methodology named Numerical Series Cryptography.

3. PRELIMINARIES

3.1 Rivest-Shamir-Adleman Cryptography

RSA stands for (Ron) Rivest – (Adi) Shamir – (Leonard) Adleman, and is one of the most well-known Public-key Cryptographic algorithms (or Asymmetric Cryptography). RSA is divided into four stages: Key Generation: To generate Private Key (to keep) and Public Key (to share). Key Distribution: Populate the network with the public key. Encryption: The sender encrypts the message with the receiver's public key. Decryption: The message is decrypted by the receiver using his or her private key.

3.2 Numerical Series Cryptography

Numerical series cryptography (NSC) [27] is easier than elliptic curve cryptography (ECC). The NSC is based on the $n\ th$ partial sum problem that is NP-complete. The main drawback of ECC is that it increases the size of the encrypted message significantly more than RSA encryption. Furthermore, the ECC algorithm is more complex and more difficult to implement than RSA, which increases the likelihood of implementation errors, thereby reducing the security of the algorithm. With NSC large symmetric keys can be used to encrypt and decrypt messages in a short execution time.

Definition 1

Suppose we have an infinite sequence of numbers: $u1, u2, u3, \dots \dots \dots, un, \dots\dots\dots$

The expression

$$u1 + u2 + u3+, \dots \dots \dots + un + \cdots \dots \dots \quad (1)$$

is called a numerical series, the numbers $u1, u2, u3, \dots\dots\dots, un, \dots$ are called the terms of the series [27].

Definition 2

The sum of a finite number of terms (the first n terms) of a series called the $n\ th$ partial sum of the series such that [26]:

$$sn = u1 + u2 + u3+, \dots \dots \dots + un \quad (2)$$

If there exists a finite limit:

$$s = limn \to \infty\ sn\ (3)$$

Then s called the sum the series in eq. (1) and we say that the series converges. If the $\lim n \to \infty\ sn$ does not exist i.e., $sn \to \infty$ as $n \to \infty$ then the series has no sum and we say this series diverges.

3.3 Adversary Threat Model

According to the capabilities of adversary V the following assumptions are made:

- Adversary V can access the public communication channel where he can retrieve, modify, replay, and inject new message and discard any message.
- The trusted third party T is protected so V cannot access the generated prime number p.

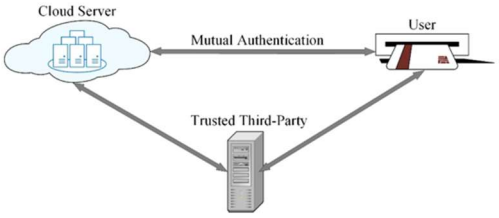

Figure 2: Proposed Scheme Architecture

4. THE PROPOSED SCHEME

Gaining users' trust requires offering security for internet services and the applications that utilize them. They must have confidence in the security of connected devices, applications, and the internet against cyber dangers. By developing a lightweight authentication protocol, this work seeks to increase the security of the authentication strategy in IoT-based environment devices. IoT devices upload their acquired data to a cloud server in an IoT-based cloud environment, and users can access the cloud servers to retrieve the data from anywhere at any time. As seen in Figure 1, the suggested authentication scheme's architecture consists of three parties. User, trustworthy third party, and cloud provider are the involved parties. In order to communicate with the cloud server, the users must register with the trusted third party.

Additionally, cloud servers must to register with a reliable third party. A trusted third party handles the mutual authentication process. For users to connect to cloud servers and request services, authentication is required in order to counter fraud, repetition, and other security measures. Therefore, in order to access the desired services from the cloud server, users must first register in the trust center, log in to the network, and then receive authentication from the trusted third-party. We go over the proposed adversary model in the sections that follow. The proposed mutual authentication protocol is then presented. The adversary model explicitly presupposes the opponent's capability in advance. The traditional Dolev-Yao model is typically followed by the adversary model of the remote authentication protocol. Recently, adversaries' skills have been improved.

We discussed our suggested method in this section, which maintains user anonymity, perfect forward secrecy, key agreement, and mutual authentication. Initialization, key generation, node registration, node authentication, and session key agreement are the main five processes. These phases are discussed in depth further below. The following subsections go over the specifics of each phase.

4.1 Initialization

In this phase, a trusted third party T generates a large prime number p.

Table 1: Notations Guide.

Notation	Description
T	Third party
U_i, U_j	ith user
ID_i	Identity of U_i
p	Large prime number
Eu_i	Public key of user i
Du_i	Private key of user i
N_i	Numerical series of user i
S_i	Partial sum of user i
t_i	Timestamp
y_i	Secret key of i
SK	Session key
m, m_i	Messages

4.2 Registration

1. Each user ui registers at the trusted third party T using his IDi to prove identity. The trusted third party encrypts the generated prime number p using the public key eui of each user ui to generate pui' as follows:

$$p\ eui \rightarrow pui\ e\ , i = 1 \ldots \ldots n \quad (4)$$

Where n is the number of users register at the trusted third party T.

2. T sends $pui\ e$ to user ui only once.

3. User ui receives the encrypted prime number $pui\ e$ from the trusted third party T.

4. User ui use his private key dui to decrypt $pui\ e$ and obtain the prime number p.

4.3 Authentication

User ui authenticates user uj as follows: Let user ui selects a numerical series $N1$ and user uj selects a different numerical series $N2$. The two infinite numerical series $N1$ and $N2$ can be chosen from a pool of infinite numerical series, the first term a and considerable number of terms k for each series are chosen using true prime number generator so that the last term k in each series is much greater than the first term a i.e., $k \gg a$. Assume that user ui chose the first term a and considerable number of terms k in numerical series $N1$. In addition, user uj use a true random generator to get the first term b and considerable number of terms r in numerical series $N2$. Assume SA is the $k\ th$ partial sum in $N1$ and SB is the $r\ th$ partial sum in $N2$.

Journal of Theoretical and Applied Information Technology
15th December 2022. Vol.100. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step 1: $ui \rightarrow uj$

1. User ui choose a numerical series.
2. User ui computes the partial sum Si of the time series $N1$ at time stamp ti.
3. User ui computes yi such that:

$$yi = Si \bmod p \quad (5)$$

4. User ui sends yi to user uj.

Step 2: $uj \rightarrow ui$

1. User uj computes the partial sum Sj of the time series $N2$ at time stamp tj.

Let uj computes yj as follows:

$$yj = Sj \bmod p \quad (6)$$

2. User uj sends yj to user uj.

Step 3: $ui \rightarrow uj$

$:\{Sij\}, uj \rightarrow ui$

$:\{Sji\}$

1. User ui obtains the shared key as follows:

$$Sij = (yi * yj) \bmod p \quad (7)$$

$$Sij = (Si \bmod p * Sj \bmod p) \bmod p \quad (8)$$

2. User ui encrypts a challenge message m and obtains message mi as follows:

$$mi = m * Sij \quad (9)$$

3. User ui sends (m, mi) to user uj.
4. User uj receives (m, mi) and use the shared key Sji as follows:

$$Sji = (yj * yi) \bmod p \quad (10)$$

$$Sji = (Sj \bmod p * Si \bmod p) \bmod p \quad (11)$$

5. User uj calculates:

$$mj = m * Sji \quad (12)$$

Note that: $Sij = Sji$

If $(mi = mj)$ then user uj verifies that user ui is communicating with him and can use the shared session key Sji for further communications within this session, otherwise the session terminates.

Similarly, user uj encrypts a challenge message m and obtains message mj as follows:

$$mj = m * Sji \quad (13)$$

6. User uj sends (m, mj) to user ui.
7. User ui receives (m, mj) and use the shared key Sij as follows:

$$mi = m * Sij \quad (14)$$

Again, if $(mi = mj)$ then user uj verifies that user ui is communicating with him and can use the shared session key Sij for further communications within this session, otherwise the session terminates. Using the shared session key users ui and uj communicate securely.

5. SECURITY ANALYSIS

This section examines the proposed scheme's security in terms of security. Burrows Abadi-Needham (BAN) logic, a well-known formal analytical technique, is used to show the validity and feasibility of the suggested system. Furthermore, an informal security analysis will be addressed in this part against certain known threats, ensuring that the proposed scheme fulfills the security needs.

5.1 Formal Analysis using BAN Logic

The BAN Logic [11] is a frequently used [12-14] analysis method for ensuring that an authentication mechanism is accurate. The BAN logic is a simple yet reliable validation logic that can be used to prove mutual authentication in an authentication protocol.

Table 2: BAN Logic Notations and Logical Rules.

Notation	Description
U_i, U_j	Two principles
M	Statement
Ui |≡ M	Ui believes statement M
Ui |~ M	Ui once said M
Ui ⇒ M	Ui controls M
Ui ▷ M	Ui sees M
#M	M is fresh
M(k)	M is encrypted with K
Ui ←k→ U	Ui and Uj have a shared key K
SK	Session key

5.1.1 BAN Logic Rules

The basic rules of the BAN logic are as followings:

1. **Message meaning rule (MMR):**

$$(Ui \mid \equiv Uj \leftarrow k \rightarrow Uj, Ui \lhd M(k))/(Ui \mid \equiv Uj \mid \sim M) \quad (15)$$

2. **Nonce verification rule (NVR):**

$$(Ui \mid \equiv \#M, Ui \mid \equiv Uj \mid \sim M)/(Ui \mid \equiv Uj \mid \equiv M) \quad (16)$$

3. **Jurisdiction rule (JR):**

$$(Ui \mid \equiv Uj \mid \Rightarrow M, Ui \mid \equiv Uj \mid \equiv M)/(Ui \mid \equiv M) \quad (17)$$

4. **Belief rule (BR):**

$$(Ui \mid \equiv (M, N))/(Ui \mid \equiv M) \quad (18)$$

5. Freshness rule (FR):

$$(Ui \mid \equiv \#M)/(Ui \mid \equiv \#(M,N)) \quad (19)$$

5.1.2 BAN Logic Goals

The goals are to show that Ui and Uj believe that they agreed on the same session key.

$$Ui \mid \equiv Ui \leftarrow SK \rightarrow Uj \quad (20)$$

$$Ui \mid \equiv Uj \mid \equiv Ui \leftarrow SK \rightarrow Uj \quad (21)$$

$$Uj \mid \equiv Ui \leftarrow SK \rightarrow Uj \quad (22)$$

$$Uj \mid \equiv Ui \mid \equiv Ui \leftarrow SK \rightarrow Uj \quad (23)$$

5.1.3 Idealized Forms

The idealized forms of the messages exchanged during the authentication can be described as follows:

$$Msg1: T \rightarrow Ui: (P)eui \quad (1)$$

$$Msg2: T \rightarrow Uj: (P)euj \quad (2)$$

$$Msg3: Ui \rightarrow Uj: yi, ti \quad (3)$$

$$Msg4: Uj \rightarrow Ui: yj, tj \quad (4)$$

5.1.4 Assumptions

The basic assumptions for the BAN logic proof are as follows:

$$A1: Ui \mid \equiv \#Ti \quad (5)$$

$$A2: Uj \mid \equiv \#Tj \quad (6)$$

$$A3: Ui \mid \equiv Uj \Rightarrow (Ui \leftarrow SK \rightarrow Uj) \quad (7)$$

$$A4: Uj \mid \equiv Ui \Rightarrow (Ui \leftarrow SK \rightarrow Uj) \quad (8)$$

$$A5: T \mid \equiv P \quad (9)$$

$$A6: T \Rightarrow P \quad (10)$$

$$A7: Ui \mid \equiv Uj \Rightarrow yi \quad (11)$$

$$A8: Uj \mid \equiv Ui \Rightarrow yj \quad (12)$$

$$A9: Ui \lhd (P)eui \quad (13)$$

$$A10: Uj \lhd (P)euj \quad (14)$$

$$A11: Ui \lhd (P(eui))\ dui \quad (15)$$

$$A12: Uj \lhd (P(euj))\ duj \quad (16)$$

5.1.5 BAN Logic Proof

$$S1. Uj \lhd (yi, p, ti) \quad (40)$$

$$S2. Uj \mid \equiv Ui \mid \sim (yi, ti) \quad (41)$$

$$S3. Uj \mid \equiv \#(yi, ti) \quad (42)$$

$$S4. Uj \mid \equiv Ui \mid \equiv (yi, ti) \quad (43)$$

$$S5. Ui \lhd (yj, p, tj) \quad (44)$$

$$S6. Ui \mid \equiv Uj \mid \sim (yj, tj) \quad (45)$$

$$S7. Ui \mid \equiv \#(yj, tj) \quad (46)$$

$$S8. Ui \mid \equiv Uj \mid \equiv (yj, tj) \quad (47)$$

$$S9. Ui \mid \equiv Uj \mid \equiv (Ui \leftarrow SK \rightarrow Uj) \quad \text{(Goal 2)}$$

$$S10. Uj \mid \equiv Ui \mid \equiv (Ui \leftarrow SK \rightarrow Uj) \quad \text{(Goal 4)}$$

The JR can be applied to S9 and S10 using A3 and A4, respectively:

$$S11. Ui \mid \equiv Ui \leftarrow SK \rightarrow Uj \quad \text{(Goal 1)}$$

$$S12. Uj \mid \equiv Ui \leftarrow SK \rightarrow Uj \quad \text{(Goal 3)}$$

Finally, the two end users/participants are mutually authenticated with each other.

5.2 Informal Analysis

We informally describe that the proposed protocol is secure against the following attacks.

Mutual Authentication

Mutual authentication between receivers and the sender is ensured by the proposed scheme. In fact, pseudo-identities are securely transmitted over the network. Because an adversary cannot compute yi or yj without the pseudo-identities, he or she cannot be validated as a genuine node (i.e., a sender or a receiver).

Replay and MITM Attack

During the node registration and authentication phases of the proposed method, an attacker could intercept communications sent between User A and User B, or between User A and the Third Party. The attacker can then attempt a replay attack by sending these signals again. However, under our approach, all communication messages contain an encrypted nonce, making it impossible for the attacker to alter them. The receiver detects the replayed message by checking the nonce if the message is replayed. As a result, our suggested technique is resistant to replay attacks.

Impersonation Attack

As previously stated, an attacker is unable to replay the messages sent by user A. Furthermore, each user should authenticate the attacker before relaying the detected data, even if the attacker claims to be a User A. The attacker cannot compute yi or yj because all nodes are preloaded with the generator S; consequently, it cannot be authenticated. As a result, the suggested system can withstand a user impersonation attempt.

Perfect Forward Secrecy

The third party and each node in the network share a secret session key. The node and the third party compute the session key together to secure data transfer. Because the parameters used in the asymmetric key generation step are unknown to the attacker, he or she cannot generate a valid session key. Even if an attacker compromises a node and obtains access to the session key, the system's security is unaffected.

Sybil Attack

An adversary can impersonate a sensor node to be authenticated as a le- Enhanced authentication and key management system for data transmission security in the IoT52 gitimate node However, in our method, sensor nodes are pre-programmed with a unique ID, and the attacker cannot deduce the identity from network traffic. Furthermore, before sending or receiving data, each node goes through the authentication process. If the opponent does not have the preloaded parameters, he or she cannot be authenticated. As a result, the suggested approach is Sybil-resistant.

Eavesdropping Attack

The suggested technique achieves reciprocal authentication, preventing an adversary from gaining access to data passing via the network during transmission. All detected data is also encrypted using symmetric session keys. This technique ensures data privacy and prohibits the attacker from disclosing the data.

6. COMPARATIVE ANALYSIS

6.1 Security Analysis

In this section, we compare the security of our proposed scheme with other related approaches [11-16]. We compared the proposed protocol to related protocols and demonstrated that it provides the requisite security by determining if the protocols can withstand specific attacks. A1—Mutual Authentication, A2—replay and man in the middle attack, A3—impersonation attack, A4—perfect forward secrecy A5—Sybil attack, and A6—eavesdropping attack were the key attacks considered in the comparison. The results in Table 3 show that our protocol can withstand a variety of assaults and has considerable security advantages over competing protocols. In the table, "Yes" means the protocol can withstand the attack, whereas "No" means it cannot.

Table 3: Comparisons of Security.

Schemes	A1	A2	A3	A4	A5	A6
[11]	×	×	×	×	✓	✓
[12]	✓	✓	✓	✓	✓	×
[13]	✓	✓	✓	✓	✓	×
[14]	✓	✓	✓	✓	✓	×
[15]	✓	✓	✓	✓	×	×
[16]	✓	✓	✓	✓	✓	×
Ours	✓	✓	✓	✓	✓	✓

6.2 Performance Analysis

Analysis of time consumption shows how much time is spent doing the cryptography procedures necessary for and during the authentication stage. The suggested protocol was compared to the same previous protocols discussed in the security analysis comparisons [11-16].

Table 4: Computational Cost Comparisons.

Schemes	$User_i$	T	Total computation
[11]	5.314 ms	0.0135 ms	5.3275 ms

[12]	4.252 ms	0.0135 ms	4.2655 ms
[13]	9.861 ms	0.0354 ms	9.8964 ms
[14]	10.874 ms	0.0313 ms	10.9053 ms
[15]	12.107 ms	0.0298 ms	12.1368 ms
[16]	9.812 ms	0.034 ms	9.8460 ms
Ours	3.189 ms	0.0135 ms	3.2025 ms

It is clear from the protocol analysis discussed above that the suggested protocol performs better in terms of computational cost and security than other relevant protocols.

7. SIMULATION RESULTS OF THE AVISPA TOOL

In order to assess the validity of the protocol, AVISPA software was employed. The most used software for the automatic validation of internet security protocols is AVISPA. Further evidence that the AVISPA is a cutting-edge tool for Internet security protocol analysis comes from experimental findings on a sizable library of Internet security protocols. No other tool, as far as we are aware, demonstrates the same degree of scope and resilience while also enjoying the same performance and scalability. OFMC, CL-AtSe, SATMC, and TA4SP are the four backends that make up AVISPA. Of these four backends, OFMC and CLATse are the most often used because, in contrast to SATMC and TA4SP, they support the implementation of "bit-wise XOR operation."

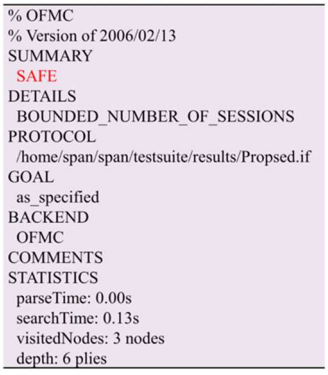

Figure 4: Security Evaluation Of Protocol In Examination By OFMC Tool

Figure 5: Security Evaluation Of Protocol In Examination By CL-Atse Tool

The suggested approach is formally validated using the On-the-Fly Model Checker (OFMC) and Constraint-Logic-based ATtack SEarcher (CL-Atse) tools. The versatile and effective CL-Atse tool examines the security of cryptographic protocols. Figures 3 and 4 show, respectively, how the OFMC and CL-AtSe tools formally validated the suggested approach. Table 5 displays the security ratings of the various authentication procedures that OFMC and CL-AtSe tools examined. The proposed method is safe when put through both tools' scrutiny, as shown in the table, whereas all other protocols are hazardous. The development of current adversary capabilities is the primary factor contributing to these methods' vulnerability.

Table 5: Security evaluation of different protocols.

Schemes	OFMC	CL-AtSe
[11]	Unsafe	Unsafe
[12]	Unsafe	Unsafe
[13]	Safe	Unsafe
[14]	Safe	Safe
[15]	Unsafe	Unsafe
[16]	Unsafe	Safe
Ours	Safe	Safe

8. CONCLUSION AND FUTURE WORK

As the Internet of Things has grown in popularity, security concerns about IoT communication have become more prominent. To secure communications in IoT-enabled WSNs, we presented a mutual authentication and session key agreement technique in this paper. Our proposed approach is resistant to known security assaults, according to an informal security review. We also used the BAN logic to formally evaluate the proposed scheme. The security analysis and findings indicate that our proposed system is safe and reliable for WSN-based IoT

applications as much as other recently established comparable methods. Future research should be devoted to further evaluate our scheme against other security attacks to ensure that it is more efficient in terms of data and communication security in addition to the communication overhead when compared to other equivalent protocols.

REFERENCES:

[1] S. Qu, L. Zhao, and Z. Xiong, "Cross-layer congestion control of wireless sensor networks based on fuzzy sliding mode control," Neural Computing and Applications, vol. 32, no. 17, pp. 13505–13520, 2020.

[2] H. Chen, Y. Chen, and L. Yang, "Intelligent early structural health prognosis with nonlinear system identification for RFID signal analysis," Computer Communications, vol. 157, pp. 150–161, 2020.

[3] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environments," IEEE Transactions on Vehicular Technology, vol. 55, no. 4, pp. 1373–1384, 2006.

[4] Z. Cheng, L. Chen, R. Comley, and Q. Tang, "Identity-based key agreement with unilateral identity privacy using pairings," in International Conference on Information Security Practice and Experience, pp. 202–213, Springer, Berlin, Heidelberg, 2006.

[5] Y. Liu and J. Cao, "An improved anonymous remote authentication protocol," in 2009 Second International Symposium on Information Science and Engineering, pp. 181–184, Shanghai, China, 2009.

[6] G. Horn and B. Preneel, "Authentication and payment in future mobile systems," in European Symposium on Research in Computer Security, pp. 277–293, Springer, 1998.

[7] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, ''A survey of Internet of Things (IoT) authentication schemes,'' Sensors, vol. 19, no. 5, p. 1141, Mar. 2019.

[8] A. K. Das, S. Zeadally, and D. He, ''Taxonomy and analysis of security protocols for Internet of Things,'' Future Gener. Comput. Syst., vol. 89, pp. 110–125, Dec. 2018.

[9] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, and L. Shu, ''Authentication protocols for Internet of Things: A comprehensive survey,'' Secure Commun. Netw., vol. 2017, pp. 1–41, Nov. 2017.

[10] M. N. Aman, K. C. Chua, and B. Sikdar, ''Mutual authentication in IoT systems using physical unclonable functions,'' IEEE Internet Things J.,vol. 4, no. 5, pp. 1327–1340, Oct. 2017, doi: 10.1109/JIOT.2017.2703088.

[11] P. Gope and B. Sikdar, ''Lightweight and privacy-preserving two-factor authentication scheme for IoT devices,'' IEEE Internet Things J., vol. 6,no. 1, pp. 580–589, Feb. 2019.

[12] C. Lyu, D. Gu, Y. Zeng, and P. Mohapatra, ''PBA: Prediction-based authentication for vehicle-to-vehicle communications,'' IEEE Trans. Dependable Secure Comput., vol. 13, no. 1, pp. 71–83, Jan. 2016.

[13] R. C. Merkle, ''A digital signature based on a conventional encryption function,'' in Proc. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 1987, pp. 369–378.

[14] G. Saldamli, L. Ertaul, and B. Kodirangaiah, ''Post-quantum cryptography on IoT: Merkle's tree authentication,'' in Proc. Int. Conf. Wireless Netw. (ICWN), 2018, pp. 35–41.

[15] X. Sun, S. Men, C. Zhao, and Z. Zhou, ''A security authentication scheme in machine-to-machine home network service,'' Secur. Commun. Netw., vol. 8, no. 16, pp. 2678–2686, Nov. 2015.

[16] M. Jan, P. Nanda, M. Usman, and X. He, ''PAWN: A payload-based mutual authentication scheme for wireless sensor networks,'' Concurrency Comput., Pract. Exper., vol. 29, no. 17, p. e3986, Sep. 2017, doi: 10.1002/cpe.3986.

[17] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, ''A privacy preserving communication protocol for IoT applications in smart homes,'' IEEE Internet Things J., vol. 4, no. 6, pp. 1844–1852, Dec. 2017.

[18] A. A. Alamr, F. Kausar, J. Kim, and C. Seo, ''A secure ECCbased RFID mutual authentication protocol for Internet of Things,'' J. Supercomput., vol. 74, no. 9, pp. 4281–4294, Sep. 2018, doi: 10.1007/s11227-016-1861-1.

[19] C.-C. Chang, H.-L. Wu, and C.-Y. Sun, ''Notes on 'secure authentication scheme for IoT and cloud servers,''' Pervas. Mobile Comput., vol. 38, pp. 275–278, Jul. 2017.

[20] S. A. Chaudhry, ''Correcting 'PALK: Password-based anonymous lightweight key agreement framework for smart grid,''' Int. J. Electr. Power Energy Syst., vol. 125, Feb. 2021, Art. no. 106529, doi: 10.1016/j.ijepes.2020.106529.

[21] S. Kalra and S. K. Sood, ''Secure authentication scheme for IoT and cloud servers,'' Pervas. Mobile Comput., vol. 24, pp. 210–223, Dec. 2015, doi: 10.1016/j.pmcj.2015.08.001.
[22] A. Maarof, M. Senhadji, Z. Labbi, and M. Belkasmi, ''Authentication protocol for securing Internet of Things,'' in Proc. 4th Int. Conf. Eng. MIS (ICEMIS), 2018, pp. 1–7.
[23] S. Hussain, S. A. Chaudhry, O. A. Alomari, M. H. Alsharif, M. K. Khan, and N. Kumar, ''Amassing the security: An ECC-based authentication scheme for Internet of drones,'' IEEE Syst. J., early access, Mar. 1, 2021, doi: 10.1109/JSYST.2021.3057047.
[24] C.-M. Chen, K.-H. Wang, W. Fang, T.-Y. Wu, and E. K. Wang, ''Reconsidering a lightweight anonymous authentication protocol,'' J. Chin. Inst. Engineers, vol. 42, no. 1, pp. 9–14, Jan. 2019.
[25] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu, and N. Kumar, ''A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers,'' J. Supercomput., vol. 74, no. 12, pp. 6428–6453, Dec. 2018.
[26] N. Chikouche, P.-L. Cayrel, E. H. M. Mboup, and B. O. Boidje, ''A privacy-preserving code-based authentication protocol for Internet of Things,'' J. Supercomput., vol. 75, no. 12, pp. 8231–8261, Dec. 2019, doi: 10.1007/s11227-019-03003-4.
[27] Lamport L. Password authentication with insecure communication. Comm the ACM. 1981;24(11):770-772.
[28] Li L-H, Lin L-C, Hwang M-S. A remote password authentication scheme for multiserver architecture using neural networks. IEEE TransNeural Netw. 2001;12(6):1498-1504.
[29] Cao X, Zhong S. Breaking a remote user authentication scheme for multi-server architecture.IEEE Comm Lett. 2006;10(8):580-581.
[30] Juang W-S. Efficient password authenticated key agreement using smart cards. Comput Secur. 2004;23(2):167-173.
[31] Ku W-C, Chuang H-M, Chiang M-H, Chang K-T, "Weaknesses of a multi-server password authenticated key agreement scheme, "in Proceedings of 2005 national computer symposium, 2005, pp. 1-5.
[32] Liao Y-P, Wang S-S. A secure dynamic ID based remote user authentication scheme for multi-server environment. Comp Stan & Inter.2009;31(1):24-29.
[33] Hsiang H-C, Shih W-K. Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment.Comp Stan & Inter. 2009;31(6):1118-1123.
[34] Amin R, Kumar N, Biswas G, Iqbal R, Chang V. A light weight authentication protocol for IoT-enabled devices in distributed cloud com-puting environment. Future Gen Comp Syst. 2018;78:1005-1019.
[35] Xue K, Hong P, Ma C. A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verificationtables for multi-server architecture.J Comp Sys Sci. 2014;80(1):195-206.