ISSN: 2584-0495 Vol. 2, Issue 5, pp.823-831

International Journal of Microsystems and IoT

ISSN: (Online) Journal homepage: https://www.ijmit.org

An Efficient Mutual Authentication Scheme for Edge Computing Enabled IIoT

Vikash Kumar, Santosh Kumar Das

Cite as: Kumar, V., & Das, S. K. (2024). An Efficient Mutual Authentication Scheme for Edge Computing Enabled IIoT. International Journal of Microsystems and IoT, 2(5), 823-831. https://doi.org/10.5281/zenodo.12780045

Published online: 15 May 2024.

DOI: https://doi.org/10.5281/zenodo.12780045

International Journal of Microsystems and IoT
Vol. 2, Issue 5, pp. 823-831, DOI: https://doi.org/10.5281/zenodo.12780045

An Efficient Mutual Authentication Scheme for Edge Computing Enabled IIoT

Vikash Kumar, Santosh Kumar Das

Department of Computer Science and Engineering, Sarala Birla University, Ranchi, India

ABSTRACT

The adoption of IIoT can revolutionize the working of industries to reduce unnecessary operational costs and increase usability and reliability, but there is the challenge of maintaining availability, scalability, and security. The collaboration of edge computing and IIoT can enhance the capabilities of industrial systems. The collaboration can resolve challenges related to latency, bandwidth, security, and real-time data processing, making industrial processes more efficient, responsive, and scalable. IIoT systems use radio frequency identification (RFID) technology to ensure that only authorized individuals or assets access specific areas, enhancing security and safety in industrial facilities. Edge computing reduces the volume of data sent from an RFID reader to a centralized cloud. RFID readers at the edge can process data locally, filtering and aggregating information before transmitting it to higher-level systems. This minimizes latency and optimizes efficiency and bandwidth usage. In this context, many authentication schemes for IIoT applications have been proposed in recent times trying to satisfy the security issue. But most of the schemes have a lot of vulnerability. This study carried out a systematic study of existing RFID authentication schemes based on Elliptic Curve Cryptography (ECC). Next, we present the system architecture, of RFID systems. Next, for IIoT applications, we developed an enhanced RFID mutual authentication system using ECC. Next, we performed a security analysis and comparison of our proposed protocol with some published work in this area. Using the AVISPA simulation tool, we finally executed a formal security verification of our proposed authentication method.

KEYWORDS

Industrial Internet of Thing, Edge computing, Radio frequency identification system, Elliptic curve cryptography, Security, Privacy, Access control, AVISPA tool.

1. INTRODUCTION

An interconnected system which is embedded with sensors, actuators, software, and other technology such as information and operational technology tools with industrial machines that make the machines able to interact, communicate, and exchange information with each other using wired or wireless technology is referred to as the Industrial Internet of Things (IIoT) [1,2,3]. IIoT systems have gained popularity with advancements in information and communication technology. IIoT systems collaborate information technology (IT) with operation technology (OT). The participating nodes in IIoT systems are usually resource-constrained in terms of energy consumption, storage capacity, processing power, and communication capacity. [4]. One of the main limitations is power, therefore extending the lifetime of the network requires an effective method that considers the power consumption of nodes. This problem gets more serious because of the high data-gathering rate and increased quantity of transmissions, especially in large-scale heterogeneous systems. There are multiple possibilities for transmitting data over the wireless medium. But it also gives attackers the ability to eavesdrop the data being broadcast or to impersonate as a different node or sensor. Conventional cryptography is not scalable for the emerging communication paradigms for the Internet of Things or cyber-physical systems. Collaboration of IIoT with Edge computing can develop a robust and productive ecosystem for industrial applications. Figure 1. shows the architecture of an edge computing-enabled IIoT system.

Edge computing plays a significant role in the Industrial Internet of Things (IIoT) by bringing computational capabilities closer to the data source, minimizing latency, improving productivity, and offering real-time data processing [7,8]. By processing sensitive data closer to the source, edge computing reduces the possibility of data leakage while being sent to a centralized cloud. This is crucial for industries where latency, security, and privacy are top priority. Communication technology is a critical component of the IIoT to connect, communicate, and share data among the systems and devices of IIoT. Fig 2. Shows the taxonomy of industrial IoT system. The parameters such as range, bandwidth, power consumption, reliability, and the specific requirements of IIoT applications decide the choice of communication technology used.

RFID stands for radio frequency identification, a rapidly growing wireless communication method that is utilised in many IIoT applications. Automated identification and authentication of personnel, tools, or equipment of IIoT system can be performed using RFID technology. IIoT systems use edge can process data locally, filtering and aggregating information before transmitting it to higher-level systems.

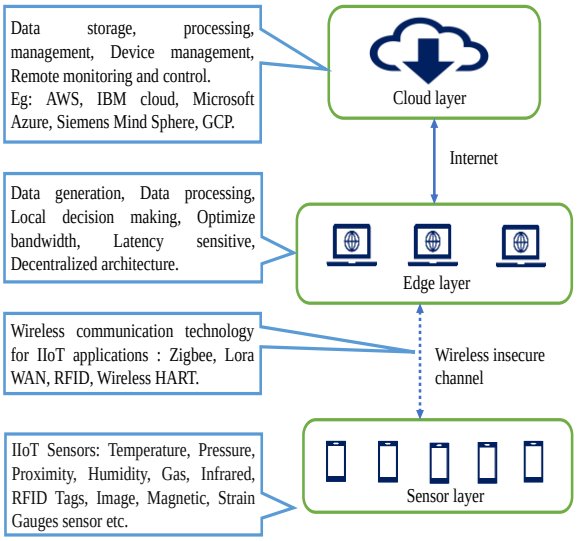

Fig. 1. Edge computing enabled IIoT architecture.

This minimizes latency, optimizes efficiency, and bandwidth usage. The RFID technology provides many advantages in terms of efficiency, automation, and access control, it also comes with specific security challenges that need to be addressed. Inadequate authentication mechanisms can make RFID systems vulnerable to unauthorized access. RFID technology to ensure that only authorized individuals or assets access specific areas, enhancing security and safety in industrial facilities [9,10]. Edge computing reduces the need to send all RFID data to a centralized cloud. RFID readers at the Strong authentication,

including mutual authentication between RFID tags and readers,

is crucial to prevent unauthorized entities from gaining access to the network. Classical cryptography-based protocol is not feasible for designing authentication mechanisms of RFID systems used in edge computing- enabled IIoT systems. Elliptic curve cryptography (ECC) [11] based authentication and encryption scheme is one of the superior cryptosystems in public key cryptosystems for the security of RFID technology. With reference to the Internet of Things, access control and authentication are crucial features that allow for safe communication between devices. Potential sources of security vulnerabilities in IIoT networks include mobility, changing network topologies, and inadequate physical security of resource-constrained devices. In a distributed and resource-constrained Internet of Things environment, it is essential to design authentication and access control protocol attacks resistant and lightweight.

The paper's remaining sections are organised as follows. Section II discussed recent existing authentication protocols developed for IoT systems. Section III discussed RFID system architecture. Section IV demonstrates the basic mathematical preliminaries of Elliptic curves cryptography. Section V proposed the improved and generalized mutual authentication scheme for IIoT consisting of the setup phase and mutual authentication phase. Section VI performed the security analysis of the proposed scheme. Section VII performed a security comparison of our scheme with some recent authentication schemes published in this area.

2. LITERATURE REVIEW

Numerous research papers have been published recently, in which some researchers have presented authentication techniques based on different cryptographic techniques while some have performed cryptanalyses of other schemes and highlighted vulnerabilities. Most of the protocols have some security issue or are not suitable for resource-constrained devices due to their complexity. Safkhani et al. [12] reviewed the level of security latest ultra-lightweight mutual authentication (MA) schemes highlighting the vulnerability of replay and desynchronization attacks. They grouped the schemes into two categories, the first is in which the tag and the reader (here the reader is connected with the backend server using a secure channel) both maintain previous data. The second is in which either the tag or the reader maintains the previous data. They proposed an enhanced MA scheme using a fresh message authentication code (MAC) function to secure against replay and desynchronization attacks. They performed security analysis through BAN Logic and Scyther tools. Izza et al. [13] cryptanalyzed Naeem et al. [14] authentication scheme and obtained vulnerability in authentication and anonymity. Next, they proposed an enhanced RFID authentication scheme for wireless body area networks (WBAN) using ECC and ECC-based digital signature (ECDS). Khorasgani et al. [15] cryptanalysis Xia et al. [16] authentication scheme and obtained vulnerability of replay, tag tracking, reader impersonation, and desynchronization attack. They proposed three improved and efficient lightweight authentication schemes. Next, they performed security analysis using Gong-Needham-Yahalom (GNY) logic and Scyther tool. Abdaoui et al. [17] proposed a unique authentication and encryption scheme by collaborating ECC and fuzzy logic. Here fuzzy logic is used to generate a random number. They evaluate their key generation method using well-defined randomness test methods like frequency tests, discrete furrier transform test and run test etc. They performed security analysis by applying some attack methods like Pollard's ρ and Baby step Giant step. Velliangiri et al. [18] proposed an enhanced and dynamic mutual authentication method for access control and secure information transferred in the vehicle networks using lightweight operations like XOR, hash function, and concatenation operations. Security analysis is performed using the AVISPA tool. Safkhani et al. [19] cryptanalysis the scheme proposed by Kumari et al. [20] and obtain vulnerability like impersonation attack, off-line estimating attack, tag traceability attack, and insider attack. Next, they proposed enhanced authentication and key agreement method using physically unclonable functions (PUF). Khan et al. [21] proposed a secure architecture for mutual authentication and encryption of medical sensor data using upgraded ECC. In this architecture first patient authentication is performed then the IoT device which is linked to the patient is activated and communicates with the cloud. The patient's biometric information has been included as a specification besides the user's name and password. The

architecture used SHA 512 to ensure integrity, Substitution-Caesar cipher, and ECC with an additional key used to ensure confidentiality and authentication. Das et al. [22] presented a certificate-based lightweight and secure key agreement and access control scheme using ECC as well as collision resistance one-way hash function for IoT applications. Security analysis is performed under both Real-Or-Random (ROR) model and the AVISPA tool. NS2 simulator is used for practical simulation. H. N. Almajed and A. S. Almogren [23] proposed a trusted and validated scheme for authentication and encryption for both encoding and mapping information to the elliptic curve. The proposed work elaborates on the importance of the security of mapping the data to the elliptic curve that is used in the encryption. He and S. Zeadally [24] proposed detailed security analysis and security requirements of RFID authentication protocols for IoT applications especially in health care using elliptic curve cryptography. The work mainly focused on the cryptanalysis of some recent work in terms of performance and security. Using biometric features, Sahoo et al. [25] recommended an ECC-based authentication system. The proposed method is prone to denial-of-service and replay attacks. Also, the computation complexity of this algorithm is high which make it unsuitable for IoT applications. A hash function and exclusive OR operations are used in Wu et al.'s [26] proposed authentication method of distributed cloud computing systems. This scheme does not ensure perfect forward secrecy and resistance against replay attack. Chall et at. [27] proposed an authentication scheme for cloud enabled cyber physical system. the scheme deals with two ways, first between a user and cloud server, and second between a cloud server and smart meter. The scheme does not ensure perfect forward secrecy. An ECC-based RFID system authentication mechanism was proposed by Dinarvand et al. [28]. This scheme is vulnerable against impersonation attack. Zhang et al. [29] proposed an ECC based authentication scheme for RFID system. This authentication scheme does not ensure confidentiality and resistance against server spoofing attack. A key management and user authentication mechanism was proposed by Wazid et al. [30] for cloud and fog enabled Internet of Things systems. The proposed protocol used hash function, bit wise exclusive OR operations. The protocol does not secure against server impersonation attack.

3. RFID SYSTEM ARCHITECTURE

The RFID system uses radio frequency for communication, and the message floating in the air can be easily eavesdropped. Figure 3 shows the architecture of RFID system. The architecture comprises three sub-sections: RFID tags, reader, and database server. The RFID reader and backed server are connected through a secure network and work as a unit. Thus, authentication takes place between the tags and the reader connected with back-end server [31]. A reader simply passes on information between tags and a backend server and does not worry about the authentication process.

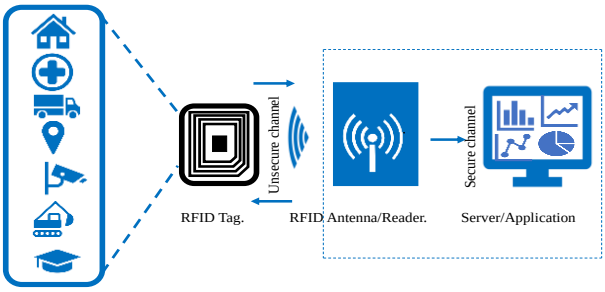

Fig. 2. RFID system architecture

An RFID tag is made up of an antenna that is connected to a microprocessor that reads and caches data. The antenna itself is made up of specialised tiny circuitry that can perform basic computations. It mainly consists of basic information like unique identifier (UID), authentication keys and sensor data and communicates this information to the reader after getting a request from the reader. RFID tags are mainly classified as active, semi-active, or passive. Active tags are powered by an internal battery, run at an ultra-high frequency and have an operating range of up to 100 meters. They are able to function over a longer distance, but not for a longer period of time. The semi-passive tags use internal battery power to keep their internal memory active but for their transmission, they depend on the power of the reader's signal [31,32]. They can operate over a longer range but are also costly and bigger as compared to passive tags. Passive tags are limited to working within very small radio ranges (a few metres) and do not have an internal power source. They are less expensive than active and semi-active tags and are powered by the reader's signal. The passive tags use the principle of induction to capture energy from the reader signal, eliminating the need for internal batteries. RFID systems typically have a very short transmission range (a few meters). Transmission happens on many different kinds of bands, ranging from ultrahigh frequencies at 860–960 MHz to low frequencies at 124–135 kHz [31,32].

3.1 Threat Model

We take for consideration the following RFID system threat model.

a. There is an insecure communication channel between the RFID tag and the RFID reader.
b. The attacker can intercept any information sent back and forth between the RFID tag and the RFID reader. He or she can replace, modify, and store all shared data, as well as replay it in future sessions.
c. There is a secure communication channel between the edge server and the reader. The edge server is secure and trusted.
d. The RFID tag is vulnerable to physical attack.
e. The ECC algorithms and one-way hash function algorithms are in public.

4. MATHEMATICAL PRELIMINARIES: ELECTIVE CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC), is a kind of public-key cryptosystem that uses the algebraic structure of elliptic curves over finite fields. It is used as replacement over traditional cryptosystems, such as RSA due to its smaller key sizes, faster computation, and strong security properties. An equation of the form $y^2 = x^3 + ax + b \pmod p$ over the finite field Fq defines an elliptic curve mathematically, where *x* and *y* are coordinates on the curve, p is a prime number, and *a* and *b* are constants such that $4a^3 + 27b^2 \neq 0 \pmod p$ [33, 34]. Next, we define a group operator " +". if we have two points P and Q in the set S then we calculate point R using the group operator "+" such as R = P+Q. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ be two points on the elliptic curve $y^2 = x^3 + ax + b \pmod p$, where $R = (x_R, y_R) = P + Q$ evaluate as follows: $x_R = (\lambda^2 - x_P - x_Q) \bmod p$, $y_R = (\lambda^2 - y_P - y_Q) \bmod p$. where $\lambda = (y_P - y_Q)/(x_P - x_Q)$ if $P \neq Q$ and $\lambda = (3x^2_P + a)/(2y_P)$ if P=Q.

4.1 Elliptic Curve Discrete Logarithmic Problem:

Given a point $P \in S_p(a, b)$, we especially have concern finding the group operations like P + P, P + P + P, P + P + P + P, P + …….+ P for a random number of times. Assume that a random number $k \in Z_P$. We can represent P + P +P+…. k times as kP. When we calculate $Q \in S_P(a, b)$ equal to k x P (Where X is not multiplication, It is a shortcut to represent repeated addition as P + P +…. K times) for a given point $P \in Sp$. To calculate k x P, the sender and the receiver use the exponential method. For example: P+P=2P, 2P+2P=4P, 4P+4P= 8, …., nP+nP= 2nP. The sender or the receiver does not calculate k x P linearly. The time complexity of calculating the k x P is in the order of logarithmic [33, 34]. But the adversary needs to calculate all the combinations of repeated addition of point P to match with point Q to recover k from the points P and Q. Adversary does not take

5. PROPOSED MUTUAL AUTHENTICATION SCHEME

In this section, we present a mutual authentication mechanism for RFID systems based on ECC for industrial Internet of things applications. The two phases of the protocol are the setup phase and the mutual authentication phase. We make the assumption that the reader and the backend database are connected via a secure channel in this protocol. Table 1 describes the different notations used in our method. In Figure 4, the proposed mutual authentication scheme is shown.

Table. 1. Notation used in our authentication scheme.

Notation	Description
q, n	Two large prime number
P	An order n generator for the elliptic curve E.
F_q	A finite field with order n and size q
E	A mathematical curve of the form y2 = x3 + axe + b (mod p), over the finite field Fq, where a, b are constants.
X_T	The identity of the tag is represented by a point on the elliptic curve E.
P_S	Public key of the edge Server
X_S	Secret key of the edge Server
r_1, r_2	Random numbers $\in Z_n$
R_1	A point generated by Server on E
R_2	A point generated by tag on E
$R1_x$	X coordinates of point R1
$R2_x$	X coordinates of point R2
$\|\|$	Bit wise OR operator
$\oplus$	Bit Wise XOR operator

5.1 Setup phase

The RFID tag saves XT as its unique identifier, while the server stores PS and XS as its public and private keys. Both the server and the tag store the curve parameters such as q, n, a, b, and P.

a. The edge server chooses its private key as a random number $X_S \in Z_n$ and evaluates its corresponding public
b. key $P_S = X_S P$. Next, The server stores X_S and P_S in the database.
c. A dynamic random point X_T on the elliptic curve E is used as the tag's unique identifier. The X_T is stored in the server as well as in the respective tag's memory. Each tag contains a unique X_T in its memory.

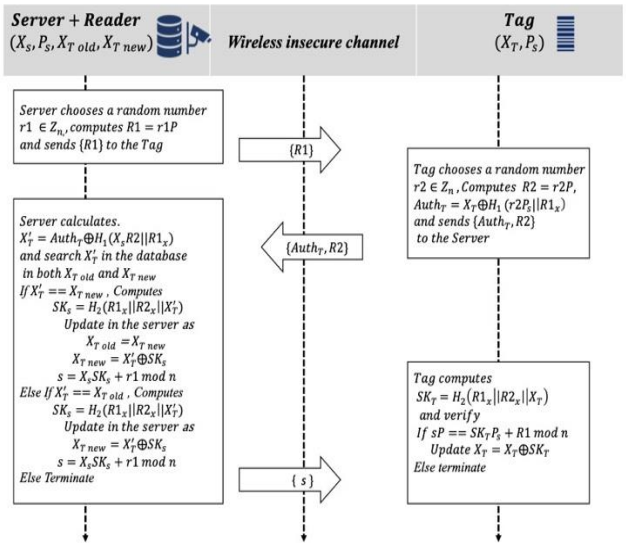

Fig. 3. Proposed mutual authentication scheme

5.2 Authentication phase

In this phase, mutual authentication is performed between the backend server and the respective RFID tag through the following step.

a. Whenever a reader gets radio frequency from any RFID tag, the authentication process starts first of all the backend server associated with the reader generates a random number $r_1 \in Z_n$ and evaluates R1= r_1P. Then the message R1 is transmitted to the tag with the help of the reader.
b. On receiving the message R_1, the tag generates a random number $r_2 \in Z_n$ and computes R2= r_2P, and

$Auth_T = X_T \oplus H_1(TK_T \| R1_x)$. Then the message ($Auth_T$ and R2) is transmitted to the server.

c. After receiving a message ($Auth_T$, R2), the server computes $X^l_T = Auth_T \oplus H_1(X_S R2 \| R1_x)$ and searches X^l_T in the database in both $X_{Told,}$ and X_{Tnew}. If X^l_T matches with X_{Tnew}, then the server computes $SK_S = H_2(R1_x \| R2_x \| X^l_T)$ and $s = X_S SK_S + r1 \bmod n$ and updates the tag's identifier as $X_{Told,} = X_{Tnew}$, $X_{Tnew} = X^l_T \oplus SK_S$. If X^l_T matches with X_{Told}, then the server computes $SK_S = H_2(R1_x \| R2_x \| X^l_T)$ and $s = X_S SK_S + r1 \bmod n$ and updates the tag's identifier as $X_{Tnew} = X^l_T \oplus SK_S$. On success, the server transmits the message {s} to the tag, on failure, the server terminates the authentication process.

d. On receiving message, the tag computes $SK_T = H_2(R1_x \| R2_x \| X_T)$ and verifies whether $sP = SK_T P_S + R1 \bmod n$. On success, authentication is over and on failure, the tag terminates the authentication process.

6. SECURITY ANALYSIS

We describe a security analysis of our suggested mutual authentication mechanism in this section. We provide scalability, forward secrecy, availability, mutual authentication, and tag anonymity in our approach. Our methodology provides strong resistance against various types of attacks, including replay, server spoofing, impersonation, location tracking, man-in-the-middle, desynchronization, tag cloning, and denial-of-service. Security analysis of the proposed scheme for the different security goals and resistance against security attack is presented below.

a. Confidentiality

In our scheme, the tag's unique identifier X_T is calculated as $X_T = Auth_T \oplus H_1(X_S R2 \| R1_x)$. Assume the adversary can obtain the {R1, R2, $Auth_T$, P_S} but without r2, it is not possible to obtain X_T.

b. Mutual Authentication

The message $Auth_T$ and R2 cannot be generated because the adversary is not able to access the tag's identifier X_T and random number r2 where R2 = r2P, $Auth_T = X_T \oplus H_1(r2P_S \| R1_x)$. The server computes $X^l_T = Auth_T \oplus H_1(X_S R2 \| R1_x)$ and authenticates the tag by verifying X^l_T with $X_{Told,}$ or X_{Tnew} in the database. Also, the adversary cannot evaluate s without knowing (X_S, r1, X_T). Where $s = X_S SK_S + r1 \bmod n$, $SK_S = H_2(R1_x \| R2_x \| X^l_T)$, $X^l_T = Auth_T \oplus H_1(X_S R2 \| R1_x)$. The tag authenticates the server by verifying whether sP is equal to $SK_T P_S + R1 \bmod n$ or not.

c. Availability

In our proposed scheme the server maintains both $X_{Told,}$ and X_{Tnew} value and the tag store updated tag's identifier X_T. The adversary cannot obtain X_T.

d. Forward Security

After each successful authentication, the tag's identifier is updated so if the adversary gets the X_T of i^{th} session. Then he/she cannot use X_T to find past session's password. The X_T is updated in both the RFID tags and backend server as $SK_S = H_2(R1_x \| R2_x \| X^l_T)$, $X_{Told,} = X_{Tnew,}$ $X_{Tnew} = X_T \oplus SK_S$.

e. Scalability

Here backend server gets the tag's unique identity is computing through $X^l_T = Auth_T \oplus H_1(X_S R2 \| R1_x)$and matching with the tag's identity in the database (in $X_{Told,}$ or X_{Tnew}). The server does not need to perform computation with each ID stored in the database. After calculating the ID as X^l_T just needed to search for the identifier in the database.

f. Tag impersonation attack

The adversary cannot produce a message ($Auth_T$ and R2) without knowing the tag's unique identifier X_T and the r2, where R2 = r2P, and $Auth_T$ $Auth_T \oplus H_1(r2P_S \| R1_x)$.

g. Server spoofing attack

If the adversary tries to impersonate itself as the legitimate server to the RFID tags. The adversary will generate a random number $r1 \in Z$ and computes R1 = r1P and transmits R1 to the tag. But the adversary is not able to generate s without X_T and X_S, where $X^l_T = Auth_T \oplus H_1(X_S R2 \| R1_x)$, $SK_S = H_2(R1_x \| R2_x \| X^l_T)$, and $s = X_S SK_S + r1 \bmod n$

h. Location tracking attack

If the adversary somehow gets the X_T and intercepts transmitted messages like {R1}, {$Auth_T$, R2}, and {s}. Still tag's location cannot be traced without knowing the server's private key X_S and two random numbers r1 and r2. Also, after each successful transaction, X_T is updated. Hence, our proposed scheme provides strong resistance against location-tracking attack.

i. Replay attack

Assume that if the adversary intercepts the transmitted message like {R1}and {s} and sends to the tag then the tag can easily identify the replay attack by verifying whether $sP == SK_T P_S + R1 \bmod n$, because each session uses a random number r2. Next, Assume the adversary tries to replay the legitimate message {$Auth_T$, R2} to the backend server. The replay attack can be easily identified by verifying the correctness of $Auth_T$ because the server generates fresh r1 for every session.

j. Tag Cloning attack

In our proposed scheme every tag has a unique identifier X_T and there is no relationship among different tag identifiers. Here, X_T is a random point on the elliptic curve. Suppose that an adversary somehow gets tag identifier X_T of a random tag. S/he cannot clone the tag's identifier X_T and cannot establish a relation among different tag's identifiers because each tag contains unique and fresh X_T.

k. De-synchronization attack

In our proposed scheme the server stores both X_{Told}, and X_{Tnew} in the database. If the adversary intercepts the message {s} and the tag does not update the new value X_T. However, a De-synchronization attack is not possible because the server matches both the value of X_{Told} and X_{Tnew}.

l. Man in the middle attack (MITM)

In our scheme, authentication is performed both ways, the server authenticates the tag and the tag authenticates the server Hence, the proposed scheme provides strong resistance against MITM attack.

7. SECURITY COMPARISION WITH SOME EXISTING WORK

We present the security comparisons of our scheme with some known authentication schemes against different security parameters such as mutual authentication, forward secrecy, resistance against tag impersonation attack, resistance against server spoofing attack, confidentiality, availability, and scalability. Abbreviations for security parameters are shown in table 2. Next the security comparisons are shown in table 3.

Table. 2. Notation used in security parameter comparison of different scheme.

Security feature (Sf)	Security features description
Sf1	Mutual authentication
Sf2	Forward secrecy
Sf3	Tag impersonation attack resistance
Sf4	Server spoofing attack resistance
Sf5	Confidentiality
Sf6	Availability
Sf7	Scalability
Sf8	Replay attack resistance

Table. 3. Comparison of existing and proposed authentication schemes.

Sf	Our	[14]	[16]	[34]	[35]	[36]	[37]	[38]	[39]
Sf1	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Sf2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
Sf3	Yes	Yes	No	Yes	No	No	Yes	Yes	Yes
Sf4	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
Sf5	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Sf6	Yes	No	No	NA	NA	NA	No	Yes	NA
Sf7	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No
Sf8	Yes	No	No	No	No	Yes	Yes	Yes	Yes

Where SF: Security feature, Yes: SF satisfied, No: Security features not satisfied, NA :Security features not applicable.

8. FORMAL SECURITY VERIFICATION USING AVISPA TOOL

We simulate our suggested method with the Automated Validation of Internet Security Protocols and Applications (AVISPA) [35, 36] tool for the formal security verification. Based on the simulation results, we conclude that our scheme is safe from replay attacks, man-in-the-middle attacks, passive assaults, and active attacks. The AVISPA is an automated software tool designed for analyzing and validating security protocols and applications. In order to identify security protocol vulnerabilities such as active attack, passive attack, man-in-the-middle attack, and replay attack, it is helpful to express the cryptographic protocols in expressive formal language. High-level protocol specification language (HLPSL) is used to express our proposed authentication protocol. HLPSL is a role-based, expressive, modular, flexible, easy-to-learn and formal language that helps to specify cryptographic and algebraic properties based on complex security protocols. The HLPSL provides declarative and semantics based on temporal logic and operational semantics based on Intermediate format (IF). HLPSL expressions can be translated into equivalent IF expressions using the HLPSL2IF translator. The AVISPA tool's backend receives the IF expressions as input. A wide range of backend security analysis tools are used, including the Tree Automata Based Protocol Analyzer (TA4SP), the On-the-fly Model Checker (OFMC), the Satisfiability Based Model Checker (SATMC), and the Constraint logic-based attack searcher (CL-AtSe).

OFMC(On-the-fly-mode-Checker): By investigating transition flow, it carries out protocol falsification and session verification for a finite number of sessions. It covers the cryptographic and algebraic features of security protocols and applies to both typed and untyped protocol models. It also offers an intuitive user interface and automatic abstraction.

CL-AtSe (Constraint –Logic-Based-Attack-Searcher): Using constraint logic programming, it conducts security verifications and protocol falsifications for a limited number of sessions. It also applies to protocol models, both typed and untyped, that are based on algebraic characteristics and cryptographic operators. It handles message concatenation associativity handling and type flow detection using a number of strong heuristics and elimination approaches.

SATMC (SAT-based Model Checker): It verifies and falsifies protocols by creating a propositional formula encoding for a finite number of sessions on a typed protocol model,

TA4SP (The Tree Automata based Protocol Analyzer): It uses standard tree language and estimates the knowledge of the intruder to performs analysis of security protocols and protocol verifications. An extension of the approximation method becomes a starting point for security verifications. TA4SP checks flaws in security protocol through under-approximation, and safety through over-approximation. It applies to unbounded number of sessions in the typed protocol model.

One of the four backend security analysis tools generates the OF (Output format). The comprehensive simulation results are displayed below.

SUMMARY: It shows the protocol is whether safe or unsafe

DETAILS: It shows the condition of the protocol which is declared safe or unsafe and different situations used for finding an attack.

PROTOCOL: It shows the protocol's name.

GOAL: The purpose of analysis shown here.

BACKEND: One of the four backend protocol's names which is used.

Finally, it shows some comments and statistics such as parse time, visited node, and depth.

8.1 AVISPA simulation code of proposed scheme

In this section we shows the basic attributes used in HLPSL language. The HLPSL code for role of edge server integrated with RFID reader , code for role of RFID tag and code for session with specified goal are presented. The output of simulation shows that our proposed mutual authentication scheme is safe and secure. Table 4 shows Basic notation with description used in HLPSL language. Table 5. shows he HLPSL code for Role of RFID server and RFID Tag. Table 6 shows the HLPSL code for Role session, goal, and output of simulation.

Table. 4. Basic notation with description used in HLPSL language.

Parameter	Description
agent	Principal names used in HLPSL code.
public key	Public keys used in HLPSL code.
symmetric key	Secret keys used in HLPSL code.
text	It represents as nonce used for messages
nat	Natural numbers in the contexts of non-message used.
const	Constants value used in the code.
hash_func	One-way cryptographic hash functions used. It is always assumed that the intruder cannot find inverse of the hash function

Table. 5. The HLPSL code for Role of RFID server and RFID Tag.

Role server (RFID Reader/Server)	**Role Tag (RFID TAG)**
role server (T, BS: agent, Hash: hash_func, Mul: hash_Func, SND, RCV:channel(dy)) played_by BS def= local State:nat, Xs, Xt, P, R1, R2, Rs, Rt: text, TKs,SKs,TKt,Auths,Autht: message init State: = 1 transition 1. State = 1 /\ RCV(start) =|> State':=2 /\ R1':=new() /\ Rs':=Mul(R1'.P) /\ SND(Rs') 2. State = 2 /\ RCV (xor (Xt, Hash(Rs.TKt')).Mul(R2'.P)) =|> State':=3 /\ TKs':=Mul(Xs.Rt) /\ Xt': = Mul(R1'.P) /\ secret (Xt,tag_identity,{T,BS}) /\ request (BS,T,verify_tag,Xt') /\ SKs': = Hash(Rs.Rt.Xt') /\ Auths':= Mul(Xs.SKs')	role tag (T, BS: agent, Hash: hash_func, Mul: hash_Func, Ps: public_key, SND,RCV:channel(dy)) played_by T def= local State:nat, Xs, Xt, P, R1, R2, Rs, Rt: text, TKs,TKt,SKs,SKt,Auths,Autht: message init State: =3 transition %Tag sending encrypted data to be authenticated. 1. State = 3 /\ RCV(Rs') =|> State': =4 /\ R2: =new() /\ Rt': = Mul(R2'.P) /\ TKt': =Mul(R2'.Ps) /\ Autht': =xor(Xt,Hash(Rs.TKt')) /\ secret (Xt,tag_identity,{T,BS}) /\ witness(T,BS,verify_tag,Xt') /\ SND(Autht'.Rt') % Verifies the data coming from reader for mutual authentication. /\ witness (BS,T,verify_server,SKs') /\ SND(Auths') end role	2. State = 4 /\ RCV(Mul(Xs.SKs')) =|> State': =6 /\ SKt':=Hash(Rs.Rt.Xt) /\ request(T,BS,verify_server,SKs') /\ Xt': = xor(Xt,SKt') end role

Table. 6. The HLPSL code for Role session, goal and output of simulation.

Role Session	**Goal**
role session (T, BS: agent, Hash: hash_func, Mul: hash_Func, Ps: public_key) def= local SND, RCV: channel(dy) composition server(T,BS,Hash,Mul,SND,RCV) /\ tag(T,BS,Hash,Mul,Ps,SND,RCV) end role role environment () def= const tag_identity,verify_tag, verify_server: protocol_id, t,bs : agent, h: hash_func, m: hash_func, p: public_key intruder_knowledge = {t,h} composition session(t,bs,h,m,p) /\ session(t,bs,h,m,p) /\ session(t,bs,h,m,p) /\ session(t,bs,h,m,p) end role	goal % Secretly shared parameters. secrecy of tag identity % Mutual authentication authentication on verify tag authentication on verify server end goal environment ()
Output	
SUMMARY SAFE DETAILS BOUNDED_NUMBER_OF_SESSIONS PROTOCOL /home/vikash/span/testsuite/results/conf.if GOAL as specified BACKEND OFMC STATISTICS TIME 202 ms parseTime 0 ms visitedNodes: 256 nodes depth: 8 plies	

9. CONCLUSION

In our research, we developed an enhanced RFID mutual authentication technique based on ECC for IIOT applications. Most of the previously proposed methods fall of satisfying the security requirements essential to make RFID systems feasible for IIoT applications. Those requirements including resistance to server spoofing attacks, mutual authentication, forward security, scalability, and impersonation attacks on tags. Although protocols that meet security requirement aren't appropriate for IIoT applications due to its resource constraint environment. Through the use of both formal and informal security analysis approaches, we have demonstrated that the proposed scheme satisfies all basic security requirements. We performed formal security verification of the proposed mutual

authentication scheme using AVISPA tool. The simulation result shows that our scheme ensure all the security requirement. Also, we made a security comparison of some previous well-known scheme with our proposed method based on the security requirements of the RFID technology. In our future work, we will perform real-time analysis of the computation cost and communication overhead of our authentication scheme.

REFERENCES

1. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in industry, 101, 1-12.
2. Munirathinam, S. (2020). Industry 4.0: Industrial internet of things (IIOT). In Advances in computers (Vol. 117, No. 1, pp. 129-164). Elsevier.
3. Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294.
4. Khan, W. Z., Rehman, M. H., Zangoti, H. M., Afzal, M. K., Armi, N., & Salah, K. (2020). Industrial internet of things: Recent advances, enabling technologies and open challenges. Computers & electrical engineering, 81, 106522.
5. Vitturi, S., Zunino, C., & Sauter, T. (2019). Industrial communication systems and their future challenges: Next-generation Ethernet, IIoT, and 5G. Proceedings of the IEEE, 107(6), 944-961.
6. Qiu, T., Chi, J., Zhou, X., Ning, Z., Atiquzzaman, M., & Wu, D. O. (2020). Edge computing in industrial internet of things: Architecture, advances and challenges. IEEE Communications Surveys & Tutorials, 22(4), 2462-2488.
7. Mao, Y., You, C., Zhang, J., Huang, K., & Letaief, K. B. (2017). A survey on mobile edge computing: The communication perspective. IEEE communications surveys & tutorials, 19(4), 2322-2358.
8. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. IEEE internet of things journal, 3(5), 637-646.
9. Weinstein, R. (2005). RFID: a technical overview and its application to the enterprise. IT professional, 7(3), 27-33.
10. Juels, A. (2006). RFID security and privacy: A research survey. IEEE journal on selected areas in communications, 24(2), 381-394.
11. Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. Computer Science Review, 47, 100530.
12. Safkhani, M., Rostampour, S., Bendavid, Y., Sadeghi, S., & Bagheri, N. (2022). Improving RFID/IoT-based generalized ultra-lightweight mutual authentication protocols. Journal of Information Security and Applications, 67, 103194.
13. Izza, S., Benssalah, M., & Drouiche, K. (2021). An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. Journal of Information Security and Applications, 58, 102705.
14. Naeem, M., Chaudhry, S. A., Mahmood, K., Karuppiah, M., & Kumari, S. (2020). A scalable and secure RFID mutual authentication protocol using ECC for Internet of Things. International Journal of Communication Systems, 33(13), e3906.
15. Khorasgani, A. A., Sajadieh, M., & Yazdani, M. R. (2022). Novel lightweight RFID authentication protocols for inexpensive tags. Journal of Information Security and Applications, 67, 103191.
16. Xiao, L., Xu, H., Zhu, F., Wang, R., & Li, P. (2020). SKINNY-based RFID lightweight authentication protocol. Sensors, 20(5), 1366.
17. Abdaoui, A., Erbad, A., Al-Ali, A. K., Mohamed, A., & Guizani, M. (2021). Fuzzy Elliptic Curve Cryptography for Authentication in Internet of Things. IEEE Internet of Things Journal, 9(12), 9987-9998.
18. Velliangiri, S., Manoharn, R., Ramachandran, S., Venkatesan, K., Rajasekar, V., Karthikeyan, P., ... & Dhanabalan, S. S. (2021). An efficient lightweight privacy-preserving mechanism for industry 4.0 based on elliptic curve cryptography. IEEE Transactions on Industrial Informatics, 18(9), 6494-6502.
19. Safkhani, M., Bagheri, N., Kumari, S., Tavakoli, H., Kumar, S., & Chen, J. (2020). RESEAP: An ECC-based authentication and key agreement scheme for IoT applications. IEEE Access, 8, 200851-200862.
20. Kumari, S., Khan, M. K., & Li, X. (2014). An improved remote user authentication scheme with key agreement. Computers & Electrical Engineering, 40(6), 1997-2012.
21. Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEE Access, 8, 52018-52027.
22. Das, A. K., Wazid, M., Yannam, A. R., Rodrigues, J. J., & Park, Y. (2019). Provably secure ECC-based device access control and key agreement protocol for IoT environment. IEEE Access, 7, 55382-55397.
23. Almajed, H. N., & Almogren, A. S. (2019). SE-ENC: A secure and efficient encoding scheme using elliptic curve cryptography. IEEE Access, 7, 175865-175878.
24. He, D., & Zeadally, S. (2014). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE internet of things journal, 2(1), 72-83.
25. Sahoo, S. S., Mohanty, S., & Majhi, B. (2020). Improved biometric-based mutual authentication and key agreement scheme using ECC. Wireless Personal Communications, 111, 991-1017.
26. Wu, F., Li, X., Xu, L., Sangaiah, A. K., & Rodrigues, J. J. (2018). Authentication protocol for distributed cloud computing: An explanation of the security situations for Internet-of-Things-enabled devices. IEEE Consumer Electronics Magazine, 7(6), 38-44.
27. Challa, S., Das, A. K., Gope, P., Kumar, N., Wu, F., & Vasilakos, A. V. (2020). Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems. Future Generation Computer Systems, 108, 1267-1286.
28. Dinarvand, N., & Barati, H. (2019). An efficient and secure RFID authentication protocol using elliptic curve cryptography. Wireless Networks, 25(1), 415-428.
29. Zheng, L., Xue, Y., Zhang, L., & Zhang, R. (2017, July). Mutual Authentication Protocol for RFID based on ECC. In 2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC) (Vol. 2, pp. 320-323). IEEE.
30. Wazid, M., Das, A. K., Kumar, N., & Vasilakos, A. V. (2019). Design of secure key management and user authentication scheme for fog computing services. Future Generation Computer Systems, 91, 475-492.
31. Juels, A. (2006). RFID security and privacy: A research survey. IEEE journal on selected areas in communications, 24(2), 381-394.
32. Weinstein, R. (2005). RFID: a technical overview and its application to the enterprise. IT professional, 7(3), 27-33.
33. Hankerson, D., Menezes, A. J., & Vanstone, S. (2006). Guide to elliptic curve cryptography. Springer Science & Business Media
34. Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. Designs, codes and cryptography, 19(2), 173-193.
35. Vigano, L. (2006). Automated security protocol analysis with the AVISPA tool. Electronic Notes in Theoretical Computer Science, 155, 61-86.
36. Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuéllar, J., ... & Vigneron, L. (2005). The AVISPA tool for the automated validation of internet security protocols and applications. In Computer Aided Verification: 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, July 6-10, 2005. Proceedings 17 (pp. 281-285). Springer Berlin Heidelberg.

Authors

Vikash Kumar received her B Tech degree in Computer Science and Engineering from Vinoba Bhave University Hazaribagh, Jharkhand, India in 2013 and M. Tech degree in Computer Science and Engineering Specialization in Information Security from Indian Institute of Technology (ISM) Dhanbad, India in 2016. He is currently pursuing PhD at the Department of Computer Science and Engineering, Sarala Birla University, Ranchi, Jharkhand, India. His areas of interest are Internet of Thing, authentication protocol design, cryptography, network security, edge computing and blockchain.

Email: vikash.iitdhanbad@gmail.com

Santosh Kumar Das received his PhD degree in Computer Science and Engineering from Indian Institute of Technology (ISM), Dhanbad, India, in 2018 and completed his M. Tech. degree in Computer Science and Engineering from Maulana Abul Kalam Azad University of Technology (erstwhile WBUT), West Bengal, India, in 2013. He is currently working as Assistant Professor at the Department of Computer Science and Engineering, Sarala Birla University, Ranchi, India. He has authored/edited more than 8 books with Springer in series as Lecture Notes in Networks and Systems, Tracts in Nature-Inspired Computing and Studies in Computational Intelligence, Taylor & Francis, Apple Academic Press, and IGI Global and has published more than 100 research papers. His research interests mainly focus on Artificial Intelligence and Blockchain.