International Journal Software Engineering and Computer Science (IJSECS)
4 (2), 2024, 553-565
Published Online August 2024 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN : 2776-4869, E-ISSN : 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v4i2.2887.

RESEARCH ARTICLE **Open Access**

Data Transfer Security in IoT Communication Based on Attribute-Based Cryptography

Adel Abidullah *
Assistant Professor, Computer Science Faculty, Kunduz University, Kunduz City, Kunduz Province, Afghanistan.
Corresponding Email: abidullahadel111@gmail.com.

Khoshal Rahman Rahmani
Assistant Professor, Computer Science Faculty, Kunduz University, Kunduz City, Kunduz Province, Afghanistan.
Email: khoshalrahman.rahmani@gmail.com.

Wali Mohammad Wadeed
Assistant Professor, Computer Science Faculty, Kunduz University, Kunduz City, Kunduz Province, Afghanistan.
Email: wadeed.walid@gmail.com.

Musawer Hakimi
Assistant Professor, Computer Science Department, Samangan University, Northeast Aybak City, Samangan Province, Afghanistan.
Email: musawer@adc.edu.in.

Received: June 29, 2024; Accepted: July 10, 2024; Published: August 1, 2024.

Abstract: Due to the drastic growth, the Internet of Things (IoT) has become an inevitable form of human life. However, IoT communication is subjected to a vast range of security breaches in the vulnerable environment, which leads to the demand for appropriate technology security issues in IoT communication. The cryptography technique exhibits effective security characteristics that promise promising results for identifying security breaches in IoT. This paper proposes attribute-based elliptical curve cryptography (ATB_ECC) to improve security in IoT communication. IoT devices perform communication to overcome security issues in IoT based on defined attributes of access points. Attributes are involved in the characteristics of trusted nodes in the network. The cryptography technique utilizes Elliptical Curve Cryptography (ECC) to transmit messages securely in the IoT environment. Through integrating attribute factors and cryptography techniques, the IoT network can distinguish variations in the active data communication and threats in the IoT network. Simulation performance is examined for different critical structures, such as low, medium, and high. The proposed ATB_ECC is examined for attack prediction scenarios considering real-time servers. The examined results stated that the proposed ATB_ECC has effectively prevented attacks, especially brute force attacks. Analysis of results stated that low-key structure exhibits minimal complexity, but the security level is minimal. A high-key structure consumes vast energy and has increased complexity, but the security is significantly improved. The comparative analysis of various key structure results illustrated that the proposed attributes-based ECC exhibits improved performance at 15% for throughput.

Keywords: Enterprise Architecture; Blockchain Technology; Artificial Intelligence; Digital Governance; E-Government.

1. Introduction

In recent years, IoT has provided a distinct number of changes in several applications such as e-life, healthcare, and marketing [1]. Several approaches have been included, such as controlled, rs, foundation, and gafoundationsifically for logical and innovative applications [2]. In the present era, IoT devices rely on several life-care and business processing systems, specifically satisfaction of individual and economic development [3]. IoT exhibits promising growth, providing prevalent and appropriate interaction with users, and is composed of heterogeneous technological development [4]. Generally, IoT smart devices offer heterogeneous and dynamic factors that utilize IoT devices based on the related dependability function, which directly links with the Qos of the adopted network system [5]. Every network relies on the IoT system involved in the system's service functionality; for complex performance functionality, more than a single service is required for performance.

As stated, IoT communication comprises modern communication technology with sensors and is involved in the exchange of information through the intelligence system. IoT communication includes several layers, including the network, middle, perception, and application layers [6][7]. For interaction with the real-world environment, the perception layer provides a communication bridge located in the IoT bottom layer. The perception layer connects several sensor devices by wired or wireless medium for data collection and network management and performs information collection with the transmission of information to a higher layer of IoT [8]. In the IoT communication application layer, it is necessary to evaluate the various fields of application for information exchange [9]-[10]. IoT devices encompass a wider variety of equipment and range from embedded small processing chips to larger servers at the high end since they require various security issues at different levels. Generally, security threats for IoT architecture deployment are presented below Low-level, Intermediate, and high-level security issues. The Cryptography technique provided an efficient data collection system for managing resources in the IoT environment [11]. However, those cryptography techniques are involved in effective data collection and management of data in IoT communication. The Cryptography technique comprises a multivariate cryptography technique with a post-quantum approach, such as the elliptical curve cryptography technique. This multi-variant cryptography technique alone is not practical for securing data in the IoT network; it requires more efficient techniques for securing data in the IoT network.

Several researchers have focused on improving the security mechanisms within IoT environments by implementing various security protocols. For instance, Raza *et al.* examined the performance of IoT communication protocols, including CoAP, MQTT, XMPP, and WebSocket, under different network load scenarios. Their comparative performance analysis concluded that the CoAP protocol outperforms others in terms of server utilization [12]. Based on smartphone applications, Kayal and Perros evaluated the performance of CoAP and MQTT protocols. Their analysis showed that MQTT offers better reliability and significant performance improvements over CoAP, especially in terms of packet loss, bandwidth utilization, and latency [13]. Further research by De Caro *et al.* examined the MQTT and CoAP protocols in terms of energy consumption and resource management, concluding that both protocols exhibit unsecured data connections with minimal data exchange security within IoT entities 0. Akatyev and James focused on evaluating the security threats in IoT systems, particularly for smart home applications. Their analysis revealed that IoT threats often include multiple factors, such as connected devices for home appliances, security devices, and monitoring systems [15]. Kaur, Rai, and Malik proposed an approach for supporting IoT systems with an appropriate security analysis scheme. Their model includes an automated process for threat modeling and risk assessment, aimed at identifying control schemes for implementing prior security measures [16].

In other research, Mun, Le Dinh, and Kwon determined the magnitude of exploitation in IoT applications and examined the backbone of operator networks and Internet Service Providers (ISPs) based on a geolocation database. This study also classified inferred IoT devices by considering the hosting sector, especially in the manufacturing sector [17]. Akatyev and James evaluated various machine learning models, including Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), and Artificial Neural Network (ANN), to predict anomalies and attacks within IoT systems [18]. To address the limitations of existing techniques, Marino, Moiso, and Petracca developed a security framework for constructing the Elliptical Curve Digital Signature Algorithm (ECDSA), which is used for efficient authentication and access control in IoT communication [19]. Raza *et al.* conducted research to develop "Lithe: Lightweight Secure CoAP for the Internet of Things," which aimed to evaluate the DTLS model compression scheme for minimal energy consumption and processing time [20]. In another study, Stergiou *et al.* constructed an IoT network to compute the round-trip time for message transmission between the sender and receiver [21].

While existing literature has focused on the construction of security schemes, their performance evaluations are often lacking. These security protocols, when implemented, often lead to increased energy consumption and higher resource utilization. Given that IoT networks typically operate with limited energy levels, it is crucial to develop appropriate techniques to enhance security while minimizing energy use. Furthermore, the literature suggests that cryptographic techniques exhibit significant potential in enhancing IoT security. Building on this, the current paper proposes an effective cryptographic technique aimed at improving security in IoT networks.

This research introduces attribute-based elliptical curve cryptography (ATB_ECC) as a method for securing data communication within IoT environments. The proposed scheme integrates attributes and factors for trusted nodes within the IoT network. Initially, ATB_ECC evaluates the attributes of nodes in the network. By examining these attributes, the network maintains a profile of each node and evaluates the attributes upon receiving a message. Once verified, the network shares cryptographic keys with the nodes. The performance of ATB_ECC was tested under three different scenarios: low-key, medium-key, and high-key structures. Simulation results indicate that ATB_ECC offers improved performance, with a 10% increase in Packet Delivery Ratio (PDR) and a 15% enhancement in throughput.

2. Research Method

2.1 Proposed ATB_ECC

In this section, presented about research methodology adopted for secure data communication in IoT communication. The proposed attribute-based encryption process consists of several stages such as information node (IN), trusted node (TN), Verification user (VU), IoT user (DU). Information nodes act as a cluster in the IoT network. Trusted node performs cryptography scheme with encryption and generation of ciphertext. Du involved in the decryption of ciphertext from the information node (IN) for the verification process. In the proposed scheme, the node located in various positions is examined based on the node location. Through the incorporation of attributes factors weights and rights are assigned to individual users in the IoT network. The VU involved in the evaluation of the signature generation based on the assigned weights. If particular, the node needs to transmit or access data in the IoT network, it is involved in ciphertext encryption and downloads those text.

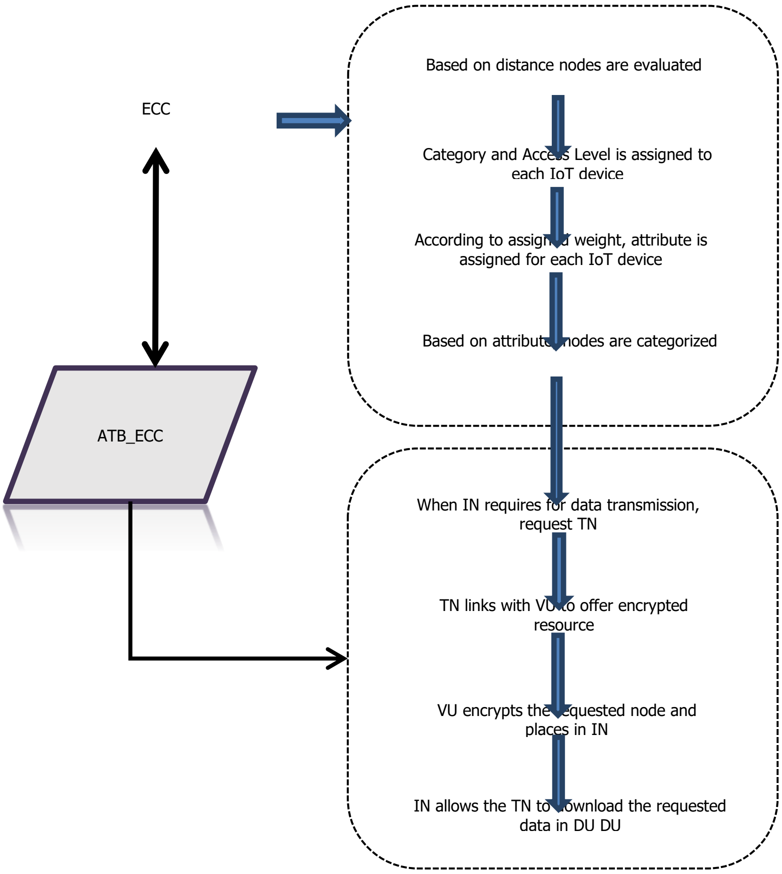
ECC
ATB_ECC
Based on distance nodes are evaluated
Category and Access Level is assigned to each IoT device
According to assigned weight, attribute is assigned for each IoT device
Based on attribute nodes are categorized
When IN requires for data transmission, request TN
TN links with VU to offer encrypted resource
VU encrypts the requested node and places in IN
IN allows the TN to download the requested data in DU DU

Figure 1. Structure of ATB_ECC

2.2 Operation of ATB_ECC

In the proposed security algorithm, the public key is generated by TA, and the master key is distributed throughout DU, VA, and TN even TN is not online. Even VA involved in the generation of the secret key with DU, with a selection of random keys such as ck$_1$,ck$_2$,…. ck$_n$ with the inclusion of subgroups of classified nodes in the network m$_1$,m$_2$,…m$_n$. With the inclusion of the ECC cryptography technique, it involved in encryption of data transmitted between n nodes in IoT communication with ciphertext Enc(m$_1$), Enc(m$_2$)… Enc(m$_n$). It involved in the creation of a signature for verification process (Vsign) with the inclusion of content key and attribute factors Aj , also it consists of several partial signatures such as U$_j$ and V$_j$. The encrypted keys and signature verification data are transmitted between VA. In VA, signature verification is performed based on the inclusion of a set of attributes A$_j$. In the attribute sets, weighted access tree WT involved in the estimation of attributes set for public key generation for the integration of ciphertext with the inclusion of content keys ck1,ck2,…. ckn. Through the inclusion of WT generates a public key for encryption and content key as ck1,ck2,…. ckn with the integration of ciphertext. VA transmits the encrypted files to IN and CT to TN. The TN generates its private key from the public key, the master key (already obtained from TA), and its attributes ai. It then downloads the requested file Enc(mj) from IN. It its private key satisfies the access policy of WT, then it can able to decrypt CT to obtain the content key ckj of the requested file. Then it decrypts the encrypted file with the content key using elliptical curve cryptography (ECC). If the private key does not match with any of the access policies of CT, it could not be able to obtain the content keys for the encrypted file. In table I abbreviation used for the construction of the algorithm is presented.

Table 1. List of Abbreviations

Notation	Meaning
Aj	Attributes set at IN
ai	Attributes of TNi
ckj	randomly chosen content key, j=1,2....n
mj	Hierarchical energy IoT nodes, j=1,2.....n
Uj	First signature part
H1,H2	Hash functions
Vsign	Node verification signature
Vj	Second signature part
SKDU	Secret Key generated by IN for TN
SKVA	Secret Key generated by TN for VU
WT	Integrated weight based access tree
CT	Ciphertext for ckj
Kpub	Public key
Kprv	Private key of TN
Kmsk	Master key
ckj , j=1,2…	Random Key

Elliptical Curve Cryptography (ECC) is performed in finite field with consideration of key size rather than traditional cryptography technique such as Diffie-Hellman, RSA to overcome time attack. ECC technique utilizes Elliptic Curve Discrete Logarithm Problem (ECDLP). Standard Efficient Cryptography (SEC) is incorporated in F_P and F_2^m for finite fields within the curve. For key generation this research utilizes curve of F_2^m . For the selected point in finite key utilizes F_2^m on curve for generation of key represented as K . $K = (m, f(x), a, b, G, n, h)$,where the parameter m represents integer lies in the F_2^m curve; the integer curve F_2^m , $f(x)$ provides the polynomial as $f(x)$; the point a, b provides elliptical curve of curve F_2^m as $E(F_2^m)$, the prime number n lies over elliptical curve with order G and h and provides cofactor of

$$h = \frac{E(F_2^m)}{n}$$

for key exchange with consideration of different energy levels. Based on defined attributes, ECC cryptography algorithm is examined with inclusion of three different elliptical curve parameter. The ATB_ECC process involved in encryption and decryption process are stated as follows:

```
Algorithm 1: Encryption with ATB_ECC in TA
Input: System parameters
Ouput: $K_{pub}, K_{msk,} SKDU$ and $SKVU$
TA generates $K_{pub}$ and $K_{msk}$ distributes to DU, VA and TN
TA generates secret key SKDU for each DU
        $SKDU = K_{msk}.H_1(DUid)$        (1)
TA generates secret key SKVA for each VA
        $SKVA = K_{msk}.H_1(VAid)$        (2)
```

```
Algorithm 2: Encryption with ATB_ECC in DU
Input: $m_j$ and $ck_j$
Output: $Enc(m_j)$
```

3. Result and Discussion

3.1 Results

Real Time (RT) server is used to verify that the proposed ATB_ECC has authorized access for data recording. Three scenarios, including RT server, BPCS, and HMI, are used to evaluate the performance of the suggested ATB_ECC. In table IV description of risk assessment model for ATB_ECC is provided.

Table 2. Description of Risk Assessment Model

Design Variables	Description
pc	The PC compromising probability
C5	The data loss probability
C6	The probability of storing data configuration for prevention and storage in local server. This offers guaranteed security to *C7.*
C7	This provides probability value of information loss
C8	This estimates the period of higher timethan the setup time.
C13	Estimate the probability of success for brute-force mysql login attack
C14	The effective password recovery forms the hash table
C15	The effective monitoring probability for disabled data from mysql
C17	The probability value of RT server
C18	The probability value of operation password leakage.
C21	The probability value of enabling of workstation

Table 3 lists the RT server's nmap port for MySQL and SSH service information. Depending on the server configuration, MySQL's authentication bypass is used for hash dumps of passwords and brute-force attacks. The Mysql data on the RT server-based risk assessment for nmap is given. The targeted service, version, and vulnerabilities taken into consideration for the ATB_ECC study are shown in table V. The RT server scenario's settings apply.

Table 3. Vulnerabilities in RT Server

Port	Service	Version	Vulnerabilities
3306/tcp	SQL	5.7.28, Protocol 10	Authentication bypass, password dump, Brute force passwords
22/tcp	Ssh	OpenSSH 7.9p1 Ubuntu 10	

In RT server attack tree for IoTsecurity assessment is approximated as shown in equation (16):

$$P[Srv - Comp] = c_{14}c_{15}(c_{16} + c_{17})(c_{11}c_{12} + c_{13}) \quad (16)$$

With equation (16) the attack probability is estimated for RT server with nmap for IoT security risk assessment. The proposed ATB_ECC offers a variety of services pertaining to IoTsecurity risk assessment in the context of Basic Process Control System (BPCS). Table 6 lists the services that are offered along with the service version for nmap for RT server scanning. Furthermore, nmap offers an RT server target because NI cRI0 9049 runs on a Linux platform. The unique open source version is predicated on vendor-specific service delivery through understanding of hardware and software. BPCS constructed an attack tree with a specific register address for the purpose of configuring control data stored in the local control drive, based on the services that were offered and the open ports.

Table 4. BPCS Vulnerabilities

Port	Service	Version	Vulnerabilities
22/tcp	ssh	OpenSSH 7.4	Brute-force SSH login
502/tcp	mdps	Modbus/TCP	Modbus Write, Stop, MITM

Modbus writes on comparable registers to increase the success rate of attack detection likelihood. The BPCS is using an open SSH port and a consecutive communication rate. By using privileged access, the BPCS controller was quickly shut down in response to an incoming DoS assault. The controller problem is rewritten with the addition of the proper software, an attack, and the assumption of adequate hardware knowledge. Finally, the DoS attack hack for Modbus adds a lot more capability by including a SYN flood attack on the SSH port. The real-time scheduling controller for attack control, or BPCS controller. It has been noted that the suggested ATB_ECC significantly improves output process and configuration performance against DoS attacks. Using BPCS attack tree design and ATB_ECC for attack probability estimate equ (17).

$$P[BPCS - Comp] = c_9[c_3c_4 + (c_1 + c_2) + a_1c_3c_4 + c_8[a_2c_7 + (c_5c_6)] \quad (17)$$

In attack scenario, HMI compromised with attack data over HMI-BPCS data as presented in table 4. The table 5 provides the HMI vulnerabilities applied for ATB_ECC algorithm is presented for analysis.

Table 5. Vulnerabilities in HMI

Port	Service	Version	Vulnerabilities
502/tcp	mdps	Modbus/TCP	Modbus write, stop
3306/tcp	MySQL	MySQL	
3389/tcp	RDP		

In proposedATB_ECC nmap provides results for HMI. Here, running windows are completely patched with inclusion of vulnerabilities identification. The developed ATB_ECC exploited efficient risk assessment for brute-force attack or via password attack. Additionally, in open port scenario malicious values are obtained with register with processing I/O knowledge configuration. In RT server user connection is based on HMI and mysql for identification of attack. It is observed that minimal number of mysql user exhibit vulnerabilities for difficult processing. It is observed that mysql eliminate user side attack through constructed HMI attack tree. The probability of HMI-BPCS data is approximated using equ (18):

$$P[HMI - BPCS] = c_5c_7 + c_{21}(c_{18} + c_{19}c_{20}) \quad (18)$$

With HMI it is observed that Man in the Middle (MITM) attack is eliminated by the RT server using proposed ATB_ECC firewall.

3.1.1 IoT Security Risk Assessment with ATB_ECC

With respect to acceptable risk assessment, the suggested ATB_ECC is evaluated for IoT security risk prediction and evaluation. The assessment of IoT failure is done using the probability values of the CPS component upper bound. The comparison of risk assessment with actual failure prediction of IoT security risks forms the basis of the risk assessment procedure. Even the suggested ATB_ECC demonstrates a reactive strategy that goes backwards to find an appropriate runtime situation. Table 8 lists the many tools, modules, and intended use of the ATB_ECC in the IoT server.

Table 6. Different Server Modules

Node	Tool	Module	Purpose
RT Server	nmap	-	Scan
RT Server	Metasploit	mysql_authbypass_hashdump	Bypass auth
RT Server	Metasploit	mysql_login	Brute- and SQL login
BPCS	nmap	-	Scan
BPCS	Metasploit	modicon_command	Start/Stop control through remote
BPCS	Metasploit	synflood	BPCS SYN Flood attack
BPCS	Metasploit	ssh_login	SSH login - Brute-force
BPCS	Metasploit	modbusclient	Manipulated data in Modbus
BPCS	Metasploit	modbusclient	Manipulated multiple data in Modbus
HMI	nmap	-	Scan
HMI	Hydra	-	RDP - Brute-force
HMI	Metasploit	modbusclient	Manipulated multiple data in Modbus

To carry out an efficient process design in risk assessment while considering a number of factors. BPCS and HMI risk evaluation and prediction are analyzed based on the designated configuration for RT server. The observed outcomes are displayed in a table. 4, table 5 and table 6. In table 7 presented about risk assessment using ATB_ECC for RT server.

Table 7. ATB_ECC Results for RT Server

Vulnerability	Notes	Tool	Result
Bypassmysql Authentication	mysql server configd to enforce authentication	Metasploit	Fail
Brute-force mysql login	Weak mysql root password used	Metasploit	Success
Linux password in hashing	Apparmor disabled for mysql	Metasploit	Success
Hashed passwords for cracked linux	root password recovered	Metasploit	Success

In table 8, ATB_ECC risk assessment performance for BPCS is provided with exploitation of tools and functional characteristics notes.

Table 8. ATB_ECC Results for BPCS

Vulnerability	Hazard Caused	Tool	Result	Notes
Modbus STOP CPU Attack	No	Metasploit	Fail	In CPU attack BPCS not supported
SYN Flood Attack to ports 22, 502	No	Metasploit	Fail	The SYN attacks does not affect communication
SSH login - Brute-force	Y/N	Metasploit	Success	user: admin, pass: "niroot" successfully identified. DoS was not significant. Integrity attack performance is reduced with utilization of software tools
Contiguous address in Modbus	No	Metasploit	Success	The process is not affected with Random write in Modbus
Contiguous address in Modbus register	No	Metasploit	Success	The communication is periodic for BPCS communication for data written in every 5 sec.

In table 9, performance of ATB_ECC for HMI is provides. The performance of is stated for HMI.

Table 9. ATB_ECC Results for HMI

Vulnerability	Risk	Exploit	Exploit	Notes
RDP - Brute-force	Yes	Hydra	Success	user: admin, pass: "reactorws" successfully deduced. HMI access gained
Contiguous address in Modbus	Yes	Metasploit	Success	Process and Modbus configuration knowledge assumed

Tables 8 through 9 show that, when RT servers are changed, the BPCS and HMI-proposed ATB_ECC performs significantly better at preventing attacks and effectively assessing the risks associated with IoT security. Information likelihood leaks initially resemble the process of configuring software. The suggested ATB_ECC offers efficient processing through c5 and c7. Second, comparable password privacy policies are enforced by different server systems, including OS, remote desktop, and database servers. According to this, c13=c14=c18. In the third stage, it is noted that the communication HMI-BPCS is higher than the tiny practice, indicating that c8 = 0. SSH offers remote configuration for RT servers. operation for the c17 = 1 remote desktop capabilities. Finally, it is noted that with c21=0, HMI provides operational annoyance. This gives the following simplified equation (19):

$$\left(c_5^2 c_{13}^2 c_{15}\right) P_c \leq 10^{-5} \qquad (19)$$

In RT server probability of failure in IoT attack offers CPS drawback. In above equation P_c presented about probability of IoT attack failure. In CPS IT security higher risk value tolerance is increases failure probability with decreased target level. Based on the simulation performed for the proposed ATB_ECC approach the performance of the proposed approach is measured at various security level. The measurement is made based on energy utilization level of nodes. In IoT communication all nodes are battery operated, hence increase in attack leads to higher security risk hence it is necessary to measure the energy consumption rate of nodes. The energy consumption rate is measured under three different scenario such as ATB_ECC level high, medium and Low. In fig 3, power level measurement of IoT nodes are comparatively presented with cipher text level.

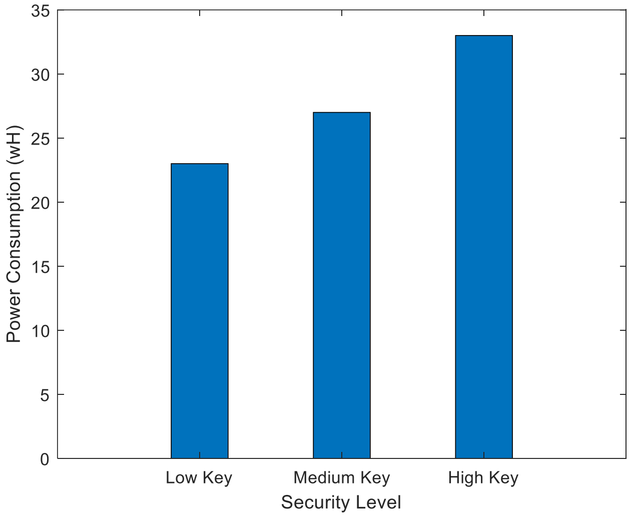

Figure 2. Security Level for proposed ATB_ECC

The power utilization level of proposed ATB_ECC provides effective power consumption rate for the IoT environment. The analysis is performed with consideration of three level security levels such as low key, medium key and high key. As explained earlier, low key consumes minimal computation time and processing time due to minimal computational complexity, medium key uses average energy and high level of energy is consumed by high key structure. From simulation analysis it is observed that low key uses energy of 21WH, medium key consumes 24.6WH and high key uses energy level of 34WH. Through observation of values it is concluded that energy consumption of high key is significantly higher than low key and medium key frame.

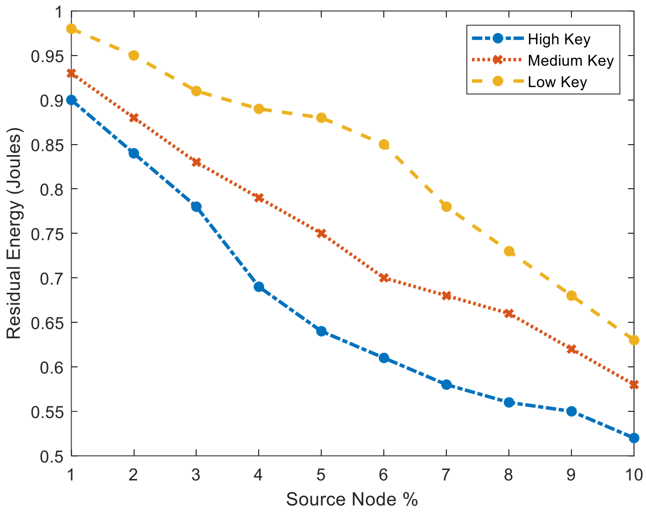

Figure 3. Energy estimation of IoT nodes

Usually, wireless communication relies on limited energy level due to battery operated nodes. In deployed IoT communication system, nodes are positioned with battery operated system, hence evaluation is measured for proposedATB_ECC with energy utilization level. The analysis is comparatively measured for low key, medium ley and high key frame. The constructed IoT network consists of 500 nodes those are converted in to percentage for evaluating the performance of IoT communication in developed ATB_ECC mechanism. In fig illustrated the energy remained in the node after implementation of keys with consideration of low key, medium key and high key. Through analysis it is observed that low key provides higher energy remaining capability. Initially, for nearby nodes nodes contains higher energy at the rate of 0.96 which is nearby normalized energy level, and it drastically reduces after certain number of source node% due to variation in the distance. Similarly, medium key provides remaining energy value of 0.91 which is significantly minimal than low key and higher than high key frame. From analysis of fig 3 and fig 4 it is observed that energy level highly relies on key structure due to computational complexity and frequent exchange of keys. However, low key exhibits higher energy remaining capability with minimal energy consumption security is higher for high keys alone.

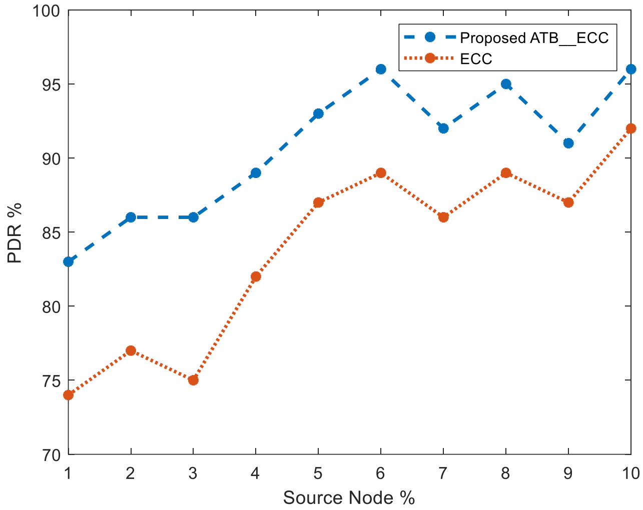

Figure 4. Comparison of PDR

In fig 4, PDR measured for proposed ATB_ECC scheme with traditional ECC scheme is presented. Packet Delivery Rate (PDR) is considered as important factor for any wireless communication medium since it provides amount of packet received by destination node. For effective communication PDR need to be higher this implies the network is highly secured. The proposedATB_ECC focused on security features in IoT communication so it is necessary to evaluate the PDR in IoT environment. The performance is comparatively examined in ECC technique. In fig 5, PDR is drastically increases with increases in source node due to location of base station. However, the proposedATB_ECC provides significant PDR rate of 97% as ECC provides PDR value of 88%. It can be concluded that proposedATB_ECC provides 10% performance enhancement rather than conventional ECC technique.

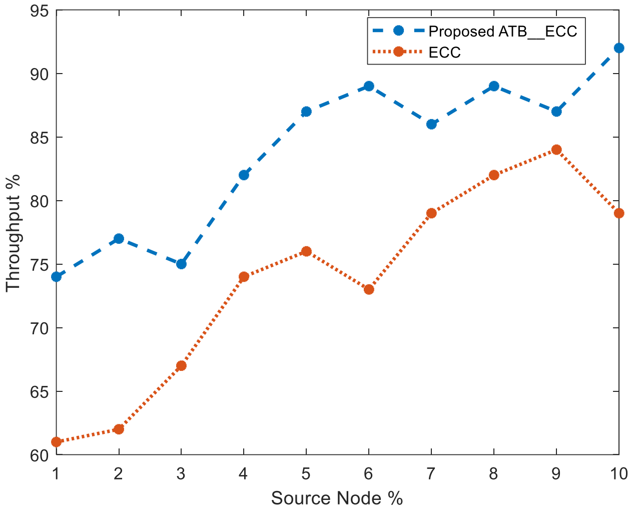

Figure 5. Comparison of Throughput

In fig 5 throughput is measured for proposed ATB_ECC scheme with traditional ECC mechanism. Throughput provides amount of data received by the network for the transmitted nodes. From simulation results it is observed that proposed ATB_ECC scheme offer higher throughput value of 97% and conventional technique provides throughput value of 83%. Through analysis it can concluded that proposed ATB_ECC provided 15% performance improvement.

3.2 Discussion

This study evaluates the effectiveness of the attribute-based elliptic curve cryptography (ATB_ECC) technique in enhancing the security of IoT networks. The simulation results demonstrate that ATB_ECC provides superior protection against security threats, mainly brute force attacks, compared to conventional elliptic curve cryptography (ECC). This study analyzed three critical structure scenarios: low, medium, and high. The low-essential structure exhibited lower energy consumption and minimal computational complexity. However, the main drawback of this structure is its lower security level, making it more vulnerable to attacks.

Conversely, the high essential structure offers better security but at the cost of significantly higher energy consumption due to increased computational complexity. The medium essential structure provides an optimal balance between security and energy consumption, making it a practical choice for deployment in energy-efficient IoT environments. In the simulations conducted, key performance metrics such as Packet Delivery Rate (PDR) and throughput were analyzed to evaluate the effectiveness of ATB_ECC. The results indicate that ATB_ECC improved PDR by 10% compared to conventional ECC, suggesting that this technique better maintains data integrity under various network conditions.

Additionally, network throughput increased by 15%, indicating higher efficiency in handling large data volumes. This study also highlights the importance of energy management in IoT networks. It is well known that all nodes in IoT networks typically rely on battery-powered resources, making energy consumption a critical factor to be carefully managed. The low-essential structure allows for significant energy savings but compromises security. Therefore, medium or high critical structures are recommended in scenarios where security is the top priority despite the higher energy consumption. In practical implementations, the trade-off between security and energy efficiency needs to be carefully considered based on the specific requirements of the IoT application.

ATB_ECC also proved effective in predicting and managing attack risks in IoT networks. Using an Autoregressive Moving Average (ARMA) model can predict attack risks more accurately, allowing for more proactive security management. Risk assessment was conducted by analyzing an Attack Control Tree (ACTree) designed explicitly for industrial scenarios. The results show that ATB_ECC can reduce potential risks by utilizing fractional differential equation-based prediction techniques, enabling early identification and mitigation of threats. The implications of this study suggest that implementing ATB_ECC can significantly enhance the security of IoT networks, particularly in defending against brute force attacks and other security threats. However, the balance between security and energy efficiency must be carefully considered in its application. Using medium-critical structures is recommended for IoT applications requiring high security and efficient energy consumption. In the future, further development of this technique could focus on improving computational efficiency for high-key structures and its application in other wireless communication networks.

4. Related Work

The security of Internet of Things (IoT) devices has become a critical concern as the number of these devices continues to grow. Numerous studies have investigated different aspects of IoT security, mainly focusing on encryption techniques, authentication protocols, and risk management strategies to mitigate vulnerabilities. The present study builds on this body of work by proposing an attribute-based elliptic curve cryptography (ATB_ECC) method to enhance security in IoT networks, focusing on balancing security and energy efficiency. Kim and Lee (2018) introduced a proxy re-encryption scheme to improve the confidentiality of data exchanged between IoT devices, particularly in scenarios where intermediary nodes may not be trusted [1]. This approach is similar to the proposed ATB_ECC in that both methods seek to secure data transmission in IoT networks through encryption. However, while Kim and Lee's study emphasizes confidentiality through re-encryption, the present study extends this concept by integrating attribute-based cryptography, which secures communication and provides a framework for access control based on specific attributes of IoT devices.

Ko, Kim, and Kim (2018) developed a platform for managing threat information in IoT environments, focusing on the real-time collection, analysis, and response to security threats [2]. This research shares a common goal with the current study regarding addressing dynamic and evolving security threats in IoT networks. However, the approach taken by Ko *et al.* is centred on threat management and intelligence, whereas the present study concentrates on strengthening the cryptographic foundation of IoT security through ATB_ECC, thereby directly preventing potential threats before they can be exploited. Azmoodeh *et al.* (2018) focused on detecting crypto-ransomware in IoT networks by analyzing energy consumption patterns [4]. Their work is closely related to the current study in that both consider energy consumption a key factor in security solutions. However, while Azmoodeh *et al.* use energy consumption as an indicator of abnormal activity, the present study uses it to optimize the cryptographic process, ensuring that security is maintained without significantly compromising the energy efficiency of IoT devices. Chen *et al.* (2019) proposed a trust architecture and reputation evaluation framework for IoT to establish trust within networks where devices may be deployed in semi-trusted or untrusted environments [5]. This is relevant to the current study, as both approaches seek to improve the reliability and security of IoT networks. The difference lies in the implementation; while Chen *et al.* focus on trust and reputation as mechanisms to secure IoT environments, the current study uses attribute-based encryption to ensure that only trusted devices can access sensitive data, thereby directly controlling access based on predefined attributes. Lin *et al.* (2018) addressed the challenge of resource management in edge computing environments by proposing a fair resource allocation system within an intrusion detection framework [6]. Their study and the present research share a common interest in optimizing resource allocation to enhance IoT security. However, Lin *et al.* focus on resource allocation to support intrusion detection, whereas the current study focuses on balancing resource usage—particularly energy consumption—within the cryptographic process itself, ensuring that IoT networks remain secure without exhausting their limited resources.

Stergiou *et al.* (2018) explored the secure integration of IoT with cloud computing, addressing the security challenges that arise when IoT systems are combined with cloud infrastructures [7]. This study complements the current research in that both address the scalability of IoT security solutions. However, while Stergiou *et al.* focus on securing data as it moves to and from the cloud, the present study focuses on securing the IoT network through a robust cryptographic scheme, ensuring that all data transmitted within the network is protected. Liu *et al.* (2018) investigated lattice-based cryptography to protect IoT devices against post-quantum threats, highlighting the need for future-proof security solutions [9]. This study and the present research emphasize the importance of forward-looking security strategies. However, while Liu *et al.* focus on the quantum resistance of cryptographic methods, the current study emphasizes the adaptability of cryptographic techniques to the unique constraints of IoT environments, such as limited energy resources and the need for lightweight security solutions. Zhang *et al.* (2018) explored mobile edge computing to reduce latency and improve energy efficiency in IoT communications [10]. Their work shares the objective of optimizing IoT performance with the present study. However, Zhang *et al.* focus on network optimization through edge computing, while the current research addresses performance improvements through an energy-efficient cryptographic framework that directly enhances the security of IoT communications. The current survey of ATB_ECC shares several commonalities with previous research, particularly in its focus on improving

IoT security. However, it distinguishes itself by integrating attribute-based cryptography with an emphasis on energy efficiency, providing a balanced approach that addresses security and resource management in IoT networks. This research contributes a unique perspective by demonstrating how cryptographic methods can be adapted to meet the specific needs of IoT environments, ensuring robust security without compromising performance.

5. Conclusion

This paper introduces an Attribute-Based Elliptic Curve Cryptography (ATB_ECC) technique designed to enhance security in IoT networks. The proposed method defines node attributes based on geographic location, hopping distance, and energy level. Nodes that meet the specified attribute conditions are designated as secure nodes within the network. The performance of the ATB_ECC approach was thoroughly evaluated across three key domains, focusing on its effectiveness in predicting and mitigating various types of attacks, including Brute-Force attacks. The evaluation results demonstrate that the ATB_ECC method substantially improves security across all tested attack scenarios. Specifically, while a low-key structure minimizes energy consumption, it offers limited protection. Conversely, a high-key structure significantly enhances security at the cost of increased energy consumption due to greater computational complexity. The IoT network employs a medium-key structure to balance security and energy efficiency. This approach effectively balances the trade-offs, resulting in a 10% improvement in the Packet Delivery Ratio (PDR) and a 15% enhancement in throughput. The findings indicate that the ATB_ECC technique enhances security within IoT networks and optimizes energy usage, making it a suitable solution for broader applications in other wireless communication networks requiring improved security measures.

References

[1] Kim, S., & Lee, I. (2018). IoT device security based on proxy re-encryption. *Journal of Ambient Intelligence and Humanized Computing, 9*(4), 1267-1273. https://doi.org/10.1007/s12652-017-0602-5

[2] Ko, E., Kim, T., & Kim, H. (2018). Management platform of threats information in IoT environment. *Journal of Ambient Intelligence and Humanized Computing, 9*(4), 1167-1176. https://doi.org/10.1007/s12652-017-0581-6

[3] Kim, W., Ko, H., Yun, H., Sung, J., Kim, S., & Nam, J. (2019). A generic Internet of things (IoT) platform supporting plug-and-play device management based on the semantic web. *Journal of Ambient Intelligence and Humanized Computing*, 1-11. https://doi.org/10.1007/s12652-019-01464-2

[4] Azmoodeh, A., Dehghantanha, A., Conti, M., & Choo, K. K. R. (2018). Detecting crypto-ransomware in IoT networks based on energy consumption footprint. *Journal of Ambient Intelligence and Humanized Computing, 9*(4), 1141-1152. https://doi.org/10.1007/s12652-017-0558-5

[5] Chen, J., Tian, Z., Cui, X., Yin, L., & Wang, X. (2019). Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing, 10*(8), 3099-3107. https://doi.org/10.1007/s12652-018-0887-z

[6] Lin, F., Zhou, Y., An, X., You, I., & Choo, K. K. R. (2018). Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of Internet of Things devices. *IEEE Consumer Electronics Magazine, 7*(6), 45-50. https://doi.org/10.1109/MCE.2018.2851723

[7] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964-975. https://doi.org/10.1016/j.future.2016.11.031

[8] Sangeetha, A. L., Bharathi, N., Ganesh, A. B., & Radhakrishnan, T. K. (2018). Particle swarm optimization tuned cascade control system in an Internet of Things (IoT) environment. *Measurement, 117*, 80-89.

[9] Liu, Z., Choo, K. K. R., & Grossschadl, J. (2018). Securing edge devices in the post-quantum internet of things using lattice-based cryptography. *IEEE Communications Magazine, 56*(2), 158-162.

[10] Zhang, K., Leng, S., He, Y., Maharjan, S., & Zhang, Y. (2018). Mobile edge computing and networking for green and low-latency Internet of Things. *IEEE Communications Magazine, 56*(5), 39-45.

[11] Guo, D., Wen, Q., Jin, Z., Zhang, H., & Li, W. (2019). Authenticated public key broadcast encryption with short ciphertexts. *Multimedia Tools and Applications, 78*(16), 23399-23414. https://doi.org/10.1007/s11042-019-7598-0

[12] Marino, F., Moiso, C., & Petracca, M. (2019). PKIoT: A public key infrastructure for the Internet of Things. *Transactions on Emerging Telecommunications Technologies, 30*(10), e3681.

[13] Bello, O., & Zeadally, S. (2019). Toward efficient smartification of the Internet of Things (IoT) services. *Future Generation Computer Systems, 92*, 663-673.

[14] Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer Systems, 89*, 110-125. https://doi.org/10.1016/j.future.2018.06.027

[15] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The Internet Society (ISOC)*, 80.

[16] Kaur, A., Rai, G., & Malik, A. (2018, January). Authentication and Context Awareness Access Control in Internet of Things: A Review. In *2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 630-635). IEEE. https://doi.org/10.1109/CONFLUENCE.2018.8443067

[17] Raza, S., Shafagh, H., Hewage, K., Hummen, R., & Voigt, T. (2013). Lithe: Lightweight secure CoAP for the internet of things. *IEEE Sensors Journal, 13*(10), 3711-3720.

[18] Kayal, P., & Perros, H. (2017, March). A comparison of IoT application layer protocols through a smart parking implementation. In *2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN)* (pp. 331-336). IEEE. https://doi.org/10.1109/ICIN.2017.7899436

[19] De Caro, N., Colitti, W., Steenhaut, K., Mangino, G., & Reali, G. (2013, November). Comparison of two lightweight protocols for smartphone-based sensing. In *2013 IEEE 20th Symposium on Communications and Vehicular Technology in the Benelux (SCVT)* (pp. 1-6). IEEE. https://doi.org/10.1109/SCVT.2013.6735994

[20] Mun, D. H., Le Dinh, M., & Kwon, Y. W. (2016, June). An assessment of internet of things protocols for resource-constrained applications. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)* (Vol. 1, pp. 555-560). IEEE. https://doi.org/10.1109/COMPSAC.2016.51

[21] Akatyev, N., & James, J. I. (2019). Evidence identification in IoT networks based on threat assessment. *Future Generation Computer Systems, 93*, 814-821. https://doi.org/10.1016/j.future.2017.10.012.