



Original Research Paper

Performance Analysis of Efficient Signcryption Schemes for Low Computing Power Devices

Anuj Kumar Singh¹, Ankit Garg², Khushboo Tripathi³, Surinder Chauhan⁴

¹Amity University Madhya Pradesh, India

Email: anujbtechcs@gmail.com

²UCRD, UIE, Chandigarh University, Mohali, Punjab, India

Email: ankitgitm@gmail.com

³Department of Computer Science & Applications, Sharda University, Greater Noida, Uttar Pradesh, India

Email: khushbootripathi.cse@gmail.com

⁴School of Computer Science, UPES, Dehradun, Uttarakhand, India

Email: surinder.chauhan01@gmail.com

Abstract - To design effective and efficient security solutions for these resource-constrained devices, a new class of computing devices termed as Low Computing Power Devices (LCPDs) has been defined. The main objective in doing so is to analyze the common security requirements, challenges, and possible security solutions for all kinds of LCPDs, so that common efficient security solutions for LCPDs can be developed. The first step in designing the appropriate security solutions for LCPDs is to choose the most efficient cryptographic system. Elliptic curve cryptography is such a cryptosystem which is suitable for LCPDs because it provides the desired level of security with smaller key size and parameters. In the second step, signcryption, which integrates the functionality of authentication and confidentiality logically in a single step, is applied along with elliptic curve cryptography for designing efficient security solutions for LCPDs. Based on the designed generic security framework for LCPDs, three security protocols one for each type of LCPD i.e. RFID tags, wireless sensors, and smart cards have been developed. Analysis of security functionalities has revealed that all these three security protocols satisfy the required security attributes and are also able to resist the attacks attempted over them. Analysis of computational cost has demonstrated that the proposed RFID security protocol reduces the computational cost for the tag by 33.33%, proposed security protocol for wireless sensors eats 50% less computation time on the gateway, and proposed smart card security protocol reduces the computational overhead on the smart card by 6% in comparison to the existing efficient protocols. Furthermore, the proposed security protocol for RFID reduces the storage cost of the tag by 8.3% and communication overhead on the tag by 8% while the developed smart card security protocol also reduces the communication cost of the smart cards by 34.28%, as compared to the existing efficient protocols.

Keywords – Signcryption, Security, Low Computing Power Devices, RFID, WSN, Smart Card.

1 INTRODUCTION

The modern computing environment has become highly ubiquitous involving heterogeneous computing devices like mainframe computers, minicomputers, desktop computers, laptops, mobile phones, tablets. Mukhopadhyay and Suryadevara [1] have mentioned that with the inception of the Internet of Things (IoT), which integrates different devices and machines with Internet connectivity, the number of computing devices is going to increase massively. In addition to the resourceful computing devices, there are devices like wireless sensor nodes, smart cards, and RFID tags that are low on computing power but are massively used in critical applications. Due to the constraints of computational resources and the wireless nature of communication, providing security to these devices has been a continuous challenge for the researchers.

1.1 Low Computing Power Devices (LCPDs)

Definition of LCPD – A Low Computing Power Device (LCPD) is defined as a computing device which possesses very low processing speed of few MIPS, clock rate of few 10s MHz, less memory of few 100s MB, and up to 1 MB flash memory.

Radio Frequency Identification (RFID) tags, wireless sensors, and smart cards are the three devices which belong to the category of LCPD, since all these three have limited processing ability, less memory, less bandwidth, and limited power supply. It is important to note that, cryptographic support for securing these LCPDs is available for each type of LCPD. Both, the symmetric key cryptographic algorithm like AES and the asymmetric key cryptographic mechanism like ECC can be used to provide security to the LCPDs. Moreover, SHA1 can also

***Corresponding Author:**

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.104

be used to facilitate the implementation of strong security mechanism by generating the hash code of an input.

A huge number of LCPDs are now being used in a variety of sensitive applications. Securing the LCPDs has been a continuous challenge due to the following constraints.

- Less Computing Capability – All the LCPDs have very little computing capability and therefore, implementing strong security mechanisms for LCPDs is a challenge.
- Limited Power Supply – Most of the versions of LCPDs requires a power source, generally a battery. Since the battery provides a limited power supply, heavy computations on the LCPDs must be avoided.
- Unreliable Communication – Typically all the LCPDs transmit and receive the data over open wireless channels that are vulnerable to many kinds of threats and attacks.

1.2 Security Requirements of LCPDs

Every computing environment has the requirement of implementing certain security attributes to ensure the desired level of security. Authentication, confidentiality, integrity, and non-repudiation are the four basic security features that must be provided to all kinds of computing environments. But, the constraints and properties of LCPDs enforce the implementation of some more security attributes.

Knospe and Pohl [2] have mined out that authentication, confidentiality, integrity, availability, and anonymity are the security attributes that are required for the systems involving RFID tags and readers. Moreover, forward security is also a necessary security attribute for RFID systems since they operate in an open wireless medium. Lopez et al. [3] have presented a detailed survey on the security requirements of WSNs and the attack on these networks. They pointed out that authorization, data freshness, self-organization, authentication, confidentiality, availability, integrity, forward security, and non-repudiation are the security features that must be implemented to secure a WSN. The security requirements of smart cards are also similar to those of RFID systems and WSNs. By analyzing the literature for smart card security it can be realized that authentication, confidentiality, integrity, forward security, and non-repudiation are the necessary security attributes for smart card based systems.

The security attributes common to all kinds of LCPDs are confidentiality, integrity, authentication, availability, forward security, and non-repudiation. However, for WSNs authorization, data freshness, and self-

organization are the three additional security attributes which need to be implemented.

1.3 Security Challenges for LCPDs

Due to the constraints of less computing capability, low power, and untrustworthy communication, the two major challenges in the way of securing LCPDs are – attacks attempted over LCPDs and selecting appropriate efficient cryptographic mechanism to provide necessary security functionalities.

1.3.1 Attacks on LCPDs

Khattab et al. [4] performed a detailed analysis over the attacks on RFID and figured out that the attacks on RFID can be classified as physical attacks, channel attacks, and system attacks. Dhakne and Chatur [5] performed a comprehensive analysis on the attacks on WSN and pointed out that these attacks can be divided into five classes– attacks based on different perspectives, attacks on authentication, attacks on layers, attacks on privacy, and other attacks. Ko and Caytiles [6] reviewed the security of smart cards and classified the attacks on smart cards as physical attacks, logical attacks, side channel attacks, and other attacks. Pippal et al. [7] mentioned that impersonation attack, password guessing attack, replay attack, and session attack can also be attempted on smart cards. The majority of attacks are common to all kinds of LCPDs. Logically, the attacks common to all LCPDs can be grouped into two broad categories – information security attacks and physical attacks. Information security attacks try to steal the confidential information or target to alter it while, in physical attacks, the LCPD is physically disabled, modified, or cloned. The work presented in this thesis focuses on securing LCPDs from the information security attacks. The information security attacks common to all kinds of LCPDs include eavesdropping, snooping, spoofing, skimming, replay attack, denial of service, and side channel attacks.

1.3.2 Choice of Cryptographic Mechanism

Due to resource constrained nature of LCPDs, it has been always challenging to select the appropriate security mechanism which satisfies all the required common information security attributes. Symmetric key cryptosystem (SKC), RSA based cryptosystem (RBC), elliptic curve cryptography (ECC), and pairing based cryptosystem (PBC) are the potential cryptographic systems which may be applied to secure the LCPDs. It can be analyzed that each cryptosystem has some advantages and weaknesses. SKC is faster than others but only satisfies the confidentiality attribute. RBC provides many security attributes but suffers from slow operations and high complexity. Similarly,

***Corresponding Author:**

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.104

ECC and PBC provide many security features but consume more time. Therefore, for securing LCPDs selecting any one cryptosystem out of SKC, RBC, ECC or PBC will not be a good idea.

Appropriate cryptographic mechanism combining the advantages of both symmetric key cryptosystem and asymmetric key cryptosystem must be devised for LCPDs which satisfies all the necessary security attributes at the same time consuming less computational cost.

1.4 Possible Security Solutions for LCPDs

The security solutions for LCPDs must be able to address the two security challenges i.e. first they must resist threats and attacks over LCPDs using appropriate countermeasures and second, they should use effective and efficient cryptographic schemes to implement these countermeasures. The various possible security solutions for LCPDs have been depicted in Figure 1.

One possible approach to develop and implement appropriate an cryptographic mechanism for LCPDs is to use hybrid cryptography. The second possible approach is to use signcryption [8] which is an integrated mechanism providing multiple security functionalities simultaneously with reduced computational cost and communication overhead.

1.4.1 Using Hybrid Cryptographic Mechanism for LCPDs

It has been identified by Jatoti et al. [48] that hybrid cryptographic mechanism is the unification of two or more cryptographic systems inheriting advantages of each of them, i.e. instead of applying a single cryptosystem, the idea is to use multiple cryptographic systems together for achieving security objectives of a system. However, from the literature survey of hybrid cryptographic schemes, it has been observed that the hybrid schemes are not able to provide all the security attributes necessary for LCPDs. Therefore, a more efficient security mechanism to secure LCPDs is required.

1.4.2 Using Signcryption for LCPDs

Signcryption given by Yuliang Zheng [9], is relatively a new approach that fulfills the functions of confidentiality and authentication simultaneously. Yuliang Zheng [9] proved that signcryption eats 58% less computational time and 85% reduced communication bandwidth, as compared to signature-then-encryption method. Many signcryption schemes have been developed by the researchers over the years. These signcryption schemes have been based on RSA or elliptic curve or pairing based cryptography. It has been already deduced that RSA cryptosystem and PBC are not suitable for LCPDs. Therefore, ECC based signcryption may be an efficient approach for securing LCPDs. The first elliptic

curve based signcryption mechanism was proposed by Zheng and Imai [10], and they proved that this ECC based signcryption consumes 58% reduced computational cost and 40% less communication bandwidth in comparison to ECC based signature-then-encryption method.

It has been revealed that the elliptic curve signcryption schemes in [11, 12, 13] are the only ECC based signcryption schemes that provide the maximum number of security features. Though, they do not satisfy availability. While the other schemes fail to satisfy two or more security attributes and hence cannot be used for securing a system. From this analysis, it can be concluded that none of these schemes is suitable to be used for LCPDs.

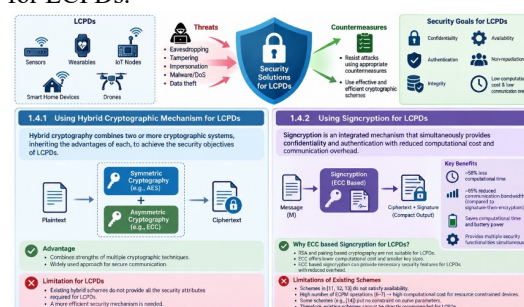


Figure 1. Possible Security Solutions for LCPDs.

The computational cost of the security schemes is proportional to the number of operations performed by them. For elliptic curve based security schemes, elliptic curve point multiplication (ECPM) operation is the most time taking operation, i.e. the time consumed by the other operations is very small in comparison to ECPM operation. Therefore, the count of ECPM operations performed by an ECC based signcryption scheme provides a clear idea about its computational cost. It has been observed that the schemes presented by Toorani and Beheshti [11] and Hagraas et al. [12] perform six ECPM operations and seven ECPM operations respectively which is very high for resource constrained environments. The scheme of Chaudhary et al. [14] puts no constraint on the size of curve parameters and therefore is not appropriate for LCPDs. With this study, it has been exposed that from computational cost viewpoint also, the signcryption schemes mentioned in Toorani and Beheshti [11], Hagraas et al. [12], and Amounas and Kinani [13] cannot be recommended for LCPDs.

If signcryption is applied for providing security to the LCPDs, then this could save more computational time, battery power, and communication bandwidth, at the same time

***Corresponding Author:**

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.104

satisfying all the necessary security functionalities for LCPDs.

2 STATEMENT OF PROBLEM

From the study of security requirements, security challenges, and possible security solutions for LCPDs, it has been witnessed that the existing security solutions have limitations since none of them satisfy the major security requirements and many of them consume more computational cost. Furthermore, efficient elliptic curve based signcryption schemes specifically for LCPDs have not been designed.

Therefore, in this research work the problem of designing efficient signcryption schemes for low computing power devices (LCPDs) which satisfy the following features has been considered:

- *Provides the necessary security attributes.*
- *Capable to counter the information security attacks on LCPDs.*
- *Consume less computational cost.*

2.1 Objectives of the Research Work

The approach to design efficient security solutions for LCPDs should be logically divided into two phases – in the first phase a generalized signcryption based security framework for LCPDs should be designed, and in the second phase the security mechanism for specific type of LCPD based on the framework proposed in the first phase should be developed. The problem defined has been divided into the following research objectives:

- To study the security requirements, challenges, and possible security solutions for LCPDs.
- To design a generalized elliptic curve signcryption based security framework for all kinds of LCPDs.
- To develop an efficient signcryption based security protocol for RFID.
- To develop an efficient signcryption based security protocol for WSNs.
- To develop an efficient signcryption based security protocol for Smart Cards.

3 ELLIPTIC CURVE SIGNCRYPTION BASED SECURITY FRAMEWORK FOR LCPDs

A security framework for LCPDs based on the concept of elliptic curve signcryption has been designed in this research work. The steps of the proposed elliptic curve signcryption based security framework have been divided into four phases – setup phase, signcryption phase, unsigncryption phase, and updating phase. There

are two parties involved in the framework, first is a LCPD, which may be an RFID tag, smart card or a sensor node and the second party may be either a user or server, which gathers information from the LCPD. It has been assumed that the LCPD and second party communicates through the insecure wireless channel.

3.1 Overview of Security Framework for LCPDs

Under the setup phase of the proposed framework, the second party selects the common system parameters, secrets, and public values. The signcryption phase implements the functionality of encryption and authentication in the message sent by the LCPD to the second party. In the unsigncryption phase, the second party decrypts the confidential data and authenticates the LCPD. Furthermore, it sends the authentication data to the LCPD for authenticating itself by the LCPD. After successful mutual authentication between the LCPD and the second party, it is necessary to update the identity of the LCPD to protect the same from unauthorized disclosure and de-synchronization attack.

3.2 Performance Analysis of the Security Framework for LCPDs

The security analysis shows that this framework satisfies mutual authentication, confidentiality, key privacy, non-repudiation, forward security, integrity, availability, and anonymity. Moreover, this framework is able to resist impersonation attack, man-in-the-middle attack, DoS attack, key-compromise attack, replay attack, de-synchronization attack, and location tracking attack.

The proposed framework consumes two ECPM operations for LCPD and three ECPM operations for the second party. Assuming 160 bit ECC parameters, AES 128, and SHA1 have been utilized in implementation in this framework, the communication cost is 736 bits for the LCPD and 567 bits for the second party while the storage cost is 1440 bits for LCPD and $2560+640m$ bits for the second party, if there are m number of LCPDs in the system.

4. ELLIPTIC CURVE SIGNCRYPTION BASED SECURITY PROTOCOL FOR RFID

Security and privacy have been a primary concern for RFID systems due to their less computational capacity. Many security solutions offering different security properties have been proposed over the years. But, a large amount of the emphasis has been given in designing secure authentication protocols for RFID, as the majority of applications implement RFID for

***Corresponding Author:**

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.104

authentication of objects by the reader or the server. Furthermore, many secure and efficient protocols based on elliptic curves have been proposed in recent years, since elliptic curve based solutions are suitable for resource constrained applications.

Recently, Dinarvand and Barati [15] presented an elliptic curve based mutual authentication protocol which offers many security features including mutual authentication, confidentiality, forward security, scalability, anonymity, availability, and integrity. They also proved that the protocol can defend against cloning, replay, de-synchronization, location tracking, masquerade, modification, and server spoofing attacks. Dinarvand and Barati [15] also compared their protocol with the related ones and showed that it takes less computational time and communication cost than others. Zheng et al. [16] designed a mutual authentication scheme based on ECC which provides confidentiality, forward security, scalability, mutual authentication, and anonymity. In addition to the security attributes mentioned, this protocol provides resistance against system internal attack, camouflage attacks, denial of service attacks, and tracking attacks. But, Zheng et al.'s protocol consumes much higher computational cost than the protocol of Dinarvand and Barati [15].

4.1 Proposed Security Protocol for RFID

An elliptic curve signcryption based security protocol for RFID (ECSSP-RFID) has been proposed in this research work. The two major communicating parties in a RFID system are tags and readers/server. In the proposed ECSSP-RFID, it presumed that the communication link between the server and the tag is wireless and insecure, while the link between the reader and the server is wired and secure. The proposed protocol has been divided into three phases: setup phase, signcryption-unsigncryption phase, and updating phase. In the set-up phase, public keys, private keys, and system parameters are generated. In signcryption-unsigncryption phase, authentication and confidentiality attributes are implemented in the transfer of messages involving the server and the tag. The tag and the server authenticate each other in this phase. After successfully authenticating each other, the server and the tag must update the unique pseudonym *ID* of the tag. Since *ID* of the tag is transmitted as plaintext in the proposed protocol, it is important to update the tag pseudonym so that it can be protected from unauthorized usage and de-synchronization attack.

4.2 Security Functionalities of ECSSP-RFID

Security analysis of the proposed ECSSP-RFID shows that it successfully provides mutual

authentication, confidentiality, non-repudiation, integrity, availability, forward security, anonymity, and scalability. Moreover, the proposed protocol can resist replay attack, impersonation attack, location tracking attack, de-synchronization attack, denial of service attack, man-in-the-middle attack, cloning attack, and key-compromise attack.

4.3 Performance Analysis of ECSSP-RFID

In the ECSSP-RFID three ECPM operations are performed by the server and two ECPM operations are performed by the tag. It has been demonstrated that it takes 0.064 sec on a 5 MHz tag to compute a single elliptic curve scalar multiplication operation so, the time consumed by the tag is 0.128 sec, the time taken by the server is 0.192 sec, and the total time taken by the proposed protocol is 0.32 sec.

The proposed elliptic curve signcryption based RFID protocol has been compared on the basis of computational cost, communication cost, storage cost, and security functionalities with the other related protocols. It has been revealed by the comparison that many RFID security protocols fail to provide some set of security functionalities and are not found suitable for an RFID system. The proposed protocol along with the protocols given by Dinarvand and Barati [15] and Zheng et al. [16] are the only protocols that provide all the necessary security functionalities.

It has been realized that both the computational cost and storage cost of the proposed protocol for the tag is less than that of Dinarvand and Barati [15] and Zheng et al. [16]. Furthermore, the tag's computational cost in the proposed protocol is least in all the related protocols which makes it attractive to be used for RFID systems. The communication cost of the proposed protocol is less than the protocol of Dinarvand and Barati [15] but slightly more than Zheng et al.'s [16] protocol. Moreover, in the proposed protocol the unique tag pseudonym *ID* is encrypted and then send through the channel, making the protocol more secure. Since the proposed protocol provides all the necessary security functionalities at the same time taking less computational cost and storage cost for the tag, it is ideal for securing an RFID system.



Figure 2. Performance analysis of ECSSP-RFID.

*Corresponding Author:

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.104

5 ELLIPTIC CURVE SIGNCRYPTION BASED SECURITY PROTOCOL FOR WSNs

Different security protocols for WSNs have been presented by different authors on the basis of available cryptographic systems with different levels of security. However, the current focus of the authors has been on developing ECC based security solutions for WSNs, since ECC based schemes are suitable for the applications involving LCPDs like wireless sensors. Recently, Zhang et al. [17] proposed key agreement and mutual authentication scheme for WSNs based on ECC, which provides mutual authentication, key privacy, key establishment, user anonymity and resistance from impersonation attack, off-line dictionary attack, insider attack, stolen verifier attack, replay attack, and compromised sensor node attack. But, Zhang's protocol takes more total computational cost and puts a lot of computational load on the gateway, as compared to the other similar protocols. A total of four ECPM operations are executed by the gateway node while, a total of ten ECPM operations are executed by the whole protocol, i.e. 40% of total computational overhead is burdened over the gateway node, which is the main disadvantage of Zhang's protocol. The total computational time and the time consumed by the gateway node can be reduced by using elliptic curve signcryption in designing security the protocol for WSNs.

5.1 Proposed Security Protocol for WSNs

An Elliptic Curve Signcryption based Security Protocol for WSN (ECSSP-WSN) has also been developed. The three parties involved in the communication are the user, sensor, and gateway. The proposed protocol has been divided into the setup phase, registration phase, and signcryption and key exchange phase. In the setup phase of the protocol, the gateway node selects the common parameters used by the system. The private and public keys of the gateway are also generated in this phase. In the registration phase, a user U is required to register himself with the gateway node. Furthermore, a sensor node S_i is also required to register itself with the gateway. In the signcryption and key establishment phase, the required security functionalities are implemented which includes confidentiality, mutual authentication, and key agreement. At the end of the execution of this phase, a secret session key is shared between the user and the sensor node.

5.2 Security Functionalities of ECSSP-WSN

The analysis of security functionalities of the proposed ECSSP-WSN has revealed that it

fulfills the security attributes of anonymity, confidentiality, forward secrecy, secure key establishment, key privacy, mutual authentication, and untraceability. Moreover, it has the capability to defend against replay attack, user impersonation, stolen verifier attack, sensor node impersonation, offline dictionary attack, and insider attack.

5.3 Performance Analysis of ECSSP-WSN

Analysis of the computational cost of ECSSP-WSN has revealed that four, two, and two ECPM operations are executed by the user, gateway, and sensor. It has been shown that, on an 8-bit Tmote Sky Sensor MSP 430 Node, with a clock rate of 8.192 MHz, and having RAM of 10 KB, it consumes 0.72 sec in completing a single ECPM operation. Based on this, the proposed protocol consumes 2.88 sec, 1.44 sec, and 1.44 sec for the user, gateway node, and the sensor node respectively.

The proposed elliptic curve signcryption based WSN security protocol has been compared with the related protocols on the basis of computational cost, communication cost, and the security functions. By this comparison, it can be observed that many schemes fail to satisfy some set of security functionalities, and therefore are not suitable for WSNs. The proposed protocol and the protocol of Zhang et al. [17] are the only two protocols that satisfy all the required security functionalities. However, it has been realized that the computational time of the gateway in ECSSP-WSN is reduced by 50% as compared to Zhang et al.'s protocol. Moreover, analysis shows that the total time consumed by the ECSSP-WSN is very less as compared to Zhang et al.'s protocol.

Therefore, the proposed ECSSP-WSN does not puts a huge computational workload on the gateway node and outperforms all the other related WSN security protocols.

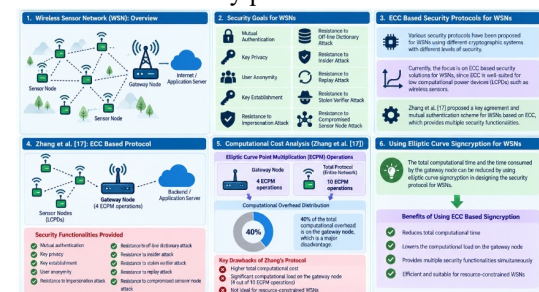


Figure 3. Performance analysis of ECSSP-WSN.

6 ELLIPTIC CURVE SIGNCRYPTION BASED SECURITY PROTOCOL FOR SMART CARDS

*Corresponding Author:

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.104

Authentication and key exchange are the primary security requirements in a user-server model. It has been identified by Zhao et al. [18] that to implement the authentication process in a client-server environment, methods based on the certificate, methods based on the password, and methods based on the identity are the three possible methods. Among these three methods, password-based methods are found to be most suitable in this environment, since password-based methods are comparatively easy to implement. To overcome the problem of offline password guessing in password-based schemes, two-tier authentication schemes have been designed in which for authentication a user has to show its credentials through smart cards and enters its password. These two-tier authentication schemes have been found stronger and secure, because even if any one of the two privates i.e. either the smart card or the password is revealed to an opponent, in that case also the scheme is secure. However, both of them must not be exposed to the opponent together.

Recently Truong et al. [19] designed an elliptic curve authentication mechanism for the multi-server environment and claimed that their schemes provide necessary security functionalities. However, Zhao et al. [18] performed a critical analysis of the scheme designed by Truong et al. [19] and showed that it fails to resist the password guessing attack and the impersonation attack.

6.1 Proposed Security Protocol for Smart Cards

An Elliptic Curve Signcryption based Security Protocol for Smart Cards (ECSSP-SC) has been presented and explained. The proposed protocol has been divided into the setup phase, registration phase, signcryption based mutual authentication phase, and update phase. The three entities participating in the proposed protocol are *USR* which is the user having a smart card, *SVR* which is the server providing services, and *RGC* the registration center. In the setup or initialization phase, the registration center *RGC* selects the common parameters for the system and publish them globally. In the registration phase, the *USR* and the server *SVR* registers themselves with the registration center *RGC*. In the signcryption based mutual authentication phase of the protocol, both *USR* and *SVR* authenticate each other. The *USR* ensures he is utilizing the services of a genuine server while the *SVR* confirms that that it is communicating with a legitimate user. This phase has been implemented by utilizing the security and performance benefits of elliptic curve based signcryption.

6.2 Security Functionalities of ECSSP-SC

Analysis of security attributes shows that the proposed smart card protocol satisfies mutual authentication, non-repudiation, forward security, anonymity, confidentiality, integrity, and availability. In addition to this, this protocol has been found secure against known key attack, replay attack, user impersonation, server impersonation, insider attack, de-synchronization attack, man-in-the-middle attack, password guessing attack.

6.3 Performance Analysis of ECSSP-SC

In ECSSP, both the smart card and the server computes two ECPM operations. Moreover, it has been figured out that by using a 2.5 GHz Intel i7 processor holding 8 GB RAM, the proposed protocol consumes 5.07 ms at both the user end and the server end. Thus, the total time consumed by the proposed protocol is 10.14ms.

It has been analyzed that many smart card security schemes either fail to satisfy one or more security attributes or fail to resist one or more security attacks. Only the schemes mentioned in Chaudhry et al. [20], Zhao et al. [18], and Xie et al. [21] other than the proposed scheme, successfully provide each required security functionality mentioned in Table 7.3 and Table 7.4. However, it is revealed that the proposed scheme eats the least computational time in comparison to all the other schemes. Thus, the ECSSP-SC is more efficient than the other related schemes and protocols for smart cards.

In addition to this, ECSSP-SC reduces the communication overhead by 34.28% as compared to Zhao et al.'s protocol [18].

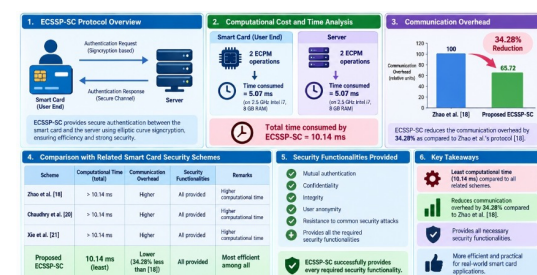


Figure 4. Performance analysis of ECSSP-SC.

7 CONCLUSION AND FUTURE SCOPE

The work presented in this thesis has systematically mined out the security requirements, security challenges, and possible security solutions for the three primarily used LCPDs i.e. RFID tags, wireless sensors, and smart cards. Based on this study, an elliptic curve signcryption based security framework has been proposed here which can be used for securing different LCPDs. It has been shown that the proposed signcryption based security framework

*Corresponding Author:

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.104

has the capability to satisfy the necessary security requirements for LCPDs.

An efficient ECSSP-RFID based on the designed framework has been developed and presented. The major advantage of this protocol is that it reduces the computational cost for the tag by 33.33%, storage overhead of the tag by 8.3%, and communication cost of the tag by 8% in comparison to the protocol presented by Dinarvand and Barati [79]. Moreover, this protocol successfully satisfies all the security features required by RFID.

The ECSSP-WSN proposed here also utilizes the designed signcryption based security framework and reduces the computational time on the gateway by 50% as compared to Zhang et al.'s protocol [97] at the same time offering all the necessary security functionalities. Similarly, the proposed ECSSP-SC has the advantage of consuming less computational cost than the other schemes. In addition to this, the ECSSP-SC reduces the bandwidth by 34.28% as compared to Zhao et al.'s protocol [98].

In the proposed framework and all the three security protocols presented in this thesis, the elliptic curve parameters of minimum size 160 bit must be chosen so that an adversary cannot solve ECDLP and ECDHP. In addition to this, AES of minimum size 128 bit must be used for encryption and decryption to ensure the security of the cipher.

The two future improvements for the research work presented in this thesis are – applying elliptic curve signcryption for designing an integrated security protocol for the internet of things (IoT) and applying hyper elliptic curve cryptography (HECC) for designing efficient signcryption based security protocols for LCPDs.

REFERENCES

- [1] Mukhopadhyay, Subhas Chandra, and Nagender K. Suryadevara. "Internet of Things: Challenges and opportunities." In *Internet of Things*, pp. 1-17. Springer, Cham, 2014.
- [2] Knospe, Heiko, and Hartmut Pohl. "RFID Security." *Information security technical report* 9, no. 4 (2004): 39-50.
- [3] Lopez, Javier, Rodrigo Roman, and Cristina Alcaraz. "Analysis of Security Threats, Requirements, Technologies and Standards in Wireless Sensor Networks." In *Foundations of Security Analysis and Design V*, pp. 289-338. Springer, Berlin, Heidelberg, 2009.
- [4] Khattab, Ahmed, Zahra Jeddi, Esmaeil Amini, and Magdy Bayoumi. "RFID Security Threats and Basic Solutions." In *RFID Security*, pp. 27-41. Springer, Cham, 2017.
- [5] Dhakne, A. R., and P. N. Chatur. "Detailed Survey on Attacks in Wireless Sensor Network." In *Proceedings of the International Conference on Data Engineering and Communication Technology*, pp. 319-331. Springer, Singapore, 2017.
- [6] Ko, Hoon, and Ronnie D. Caytiles. "A Review of Smartcard Security Issues." *Journal of Security Engineering* 8, no. 3 (2011): 359-370.
- [7] Pippal, Ravi Singh, C. D. Jaidhar, and Shashikala Tapaswi. "Security Issues in Smart Card Authentication Scheme." *International Journal of Computer Theory and Engineering* 4, no. 2 (2012): 206.
- [8] Zheng, Yuliang. "Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)." In *Annual International Cryptology Conference*, pp. 165-179. Springer, Berlin, Heidelberg, 1997.
- [9] Jatoti, Piyar Ali, Aftab A. Memon, Bhawani Shankar Chowdhry, M. Ghazanfar Ullah, and Shiraz Latif. "An Efficient Hybrid Cryptographic Algorithm, Consuming Less Time for Exchanging Information in Wireless Sensor Networks." *Wireless Personal Communications* 85, no. 2 (2015): 449-462.
- [10] Zheng, Yuliang, and Hideki Imai. "How to Construct Efficient Signcryption Schemes on Elliptic Curves." *Information processing letters* 68, no. 5 (1998): 227-233.
- [11] Toorani, Mohsen, and Ali A. Beheshti. "An elliptic curve-based signcryption scheme with forward secrecy." *arXiv preprint arXiv:1005.1856* (2010).
- [12] Hagraas, Esam A., Doaa El-Saied, and Hazem H. Aly. "A New Forward Secure Elliptic Curve Signcryption Key Management (FS-ECSKM) Scheme for Heterogeneous Wireless Sensor Networks." *International Journal of Computer Science and Technology* 2, no. 2 (2011): 19-23.
- [13] Amounas, Fatima, and El Hassan Kinani. "An Efficient Signcryption Scheme Based on the Elliptic Curve Discrete Logarithm Problem." *International Journal of Information and Network Security* 2, no. 3 (2013): 253.
- [14] Chaudhry, Shehzad Ashraf, Mohammad Sabzinejad Farash, Husnain Naqvi, and Muhammad Sher. "A Secure and Efficient Authenticated Encryption for Electronic Payment Systems using Elliptic Curve

***Corresponding Author:**

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.104

- Cryptography." *Electronic Commerce Research* 16, no. 1 (2016): 113-139.
- [15] Dinarvand, Negin, and Hamid Barati. "An Efficient and Secure RFID Authentication Protocol using Elliptic Curve Cryptography." *Wireless Networks* 25, no. 1 (2019): 415-428.
- [16] Zheng, Lijuan, Yujuan Xue, Linhao Zhang, and Rui Zhang. "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, 2017.
- [17] Zhang, Ke, Kai Xu, and Fushan Wei. "A Provably Secure Anonymous Authenticated Key Exchange Protocol Based on ECC for Wireless Sensor Networks." *Wireless Communications and Mobile Computing* 2018 (2018).
- [18] Zhao, Yan, Shiming Li, and Liehui Jiang. "Secure and Efficient User Authentication Scheme Based on Password and Smart Card for Multiserver Environment." *Security and Communication Networks* 2018 (2018).
- [19] Truong, Toan-Thinh, Minh-Triet Tran, Anh-Duc Duong, and Isao Echizen. "Provable Identity Based User Authentication Scheme on ECC in Multi-Server Environment." *Wireless Personal Communications* 95, no. 3 (2017): 2785-2801.
- [20] Chaudhry, Shehzad Ashraf, Husnain Naqvi, Khalid Mahmood, Hafiz Farooq Ahmad, and Muhammad Khurram Khan. "An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography." *Wireless Personal Communications* 96, no. 4 (2017): 5355-5373.
- [21] Xie, Qi, Duncan S. Wong, Guilin Wang, Xiao Tan, Kefei Chen, and Liming Fang. "Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol with Extended Security Model." *IEEE Transactions on Information Forensics and Security* 12, no. 6 (2017): 1382-1392.

***Corresponding Author:**

Received: 25th July, 2026 | Revised: 26th August, 2026 | Accepted: 30th August, 2026 | Available Online: 2nd September, 2026

(DOI): 10.70102/AEJ.2026.18.4s.104