iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VIII Month of publication: August 2025

DOI: https://doi.org/10.22214/ijraset.2025.73590

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VIII Aug 2025- Available at www.ijraset.com

Enhanced Text Security Using Fernet Cipher and Power Associative Loop-Based S-Box

Dwarampudi Pavani[1], Dr. Dasari Haritha[2], Mellam Aruna[3]
[1]*M. Tech, CSE Department, UCEK, JNTU Kakinada, Andhra Pradesh, India*
[2]*Professor, CSE Department, UCEK, INTU Kakinada, Andhra Pradesh, India*
[3]*Assistant Professor, CSE Department, UCEK, INTU Kakinada, Andhra Pradesh, India*

Abstract: Using Base64 encoding, Fernet encryption, and ZIP compression. To increase encryption strength, it suggests a unique S-Box construction based on power associative loops. Although Base64 and Fernet guarantee data security, their cryptographic structures are weak. Although it doesn't support effective compression on its own, the S-Box improves security. The necessity of combining optimal compression with robust encryption is a significant research gap. The study assesses the trade-offs between performance and computational complexity in this integration. Additionally, it looks at adaptability to various languages and text formats. Tests of cryptographic strength using differential probability, avalanche effect, and nonlinearity reveal enhanced security with ECC support.

Keywords: Elliptic Curve Cryptography, Fernet Cipher, Power Associative Loop, S-Box Construction, Secure Communication, Nonlinear Cryptographic Functions, Encryption, Text Data Protection, and Enhanced Text Security.

I. INTRODUCTION

Because of the rise in cyberthreats and data breaches, text data security is essential in today's digital environment. Sensitive data must be encrypted to preserve its integrity and confidentiality. Stronger cryptographic techniques are required to withstand increasingly complex attacks as computing power increases.

This study uses a Power Associative Loop-based S-Box, Base64 encoding, and Fernet encryption. Creating a strong framework for text data protection is the goal. Both symmetric and asymmetric traditional encryption models have advantages and disadvantages. Although symmetric encryption is quick, key management can be difficult. Although asymmetric encryption is safe, it requires a lot of processing power. Efficiency and security are improved by a hybrid model that incorporates multiple encryption techniques. This study suggests a sophisticated method that makes use of encryption, substitution, and encoding techniques.

A. The Need For Secure Text Encryption

Text data, which is utilised in cloud storage, messaging apps, and emails, is essential to digital communication. Stronger encryption techniques are crucial for protecting data in light of changing cyberthreats. Computational complexity is frequently the only focus of traditional encryption. Multiple security layers, however, make a system more resistant to cryptanalysis. Text data must be prepared using Base64 encoding prior to encryption.

It transforms text into a format that is structured and compatible with all platforms. Base64 guarantees data consistency but does not conceal content like encryption does. This keeps a variety of encryption systems compatible. In secure encryption workflows, Base64 serves as a dependable preprocessing step. The overall security and effectiveness of text data protection are improved by its integration.

B. Integrating Multiple Encryption Techniques

This study presents an integrated encryption framework that uses three essential elements—Base64 encoding, Fernet cryptography, and a Power Associative Loop-based S-Box—to improve text security. This combination ensures high security and effectiveness in text encryption by offering a multi-layered defence mechanism.

1) Base64 Encoding: Transforms text into a format that is compatible with all devices. manages non-ASCII text and special characters. increases the efficiency of encryption by reducing the complexity of the character set.
2) Fernet Cryptography: A symmetric encryption technique that guarantees the privacy of data. For message integrity, HMAC (Hash-based Message Authentication Code) is used. offers simplicity and resilience by preventing unwanted changes to encrypted data.

3) S-Box based on Power Associative Loops: Block cyphers employ S-Boxes to introduce nonlinearity and confusion. S-Box based on Power Associative Loops enhances encryption security. It strengthens defences against avalanche and high nonlinearity cryptanalytic attacks.

C. Applications Of Secure Text Encryption: The Need For Secure Text Encryption Extends Across Various Domains, Including

1) Secure Communication: Safeguarding private communications via email and instant messaging apps.
2) Cloud Storage Security: Preventing unwanted access and guaranteeing the privacy of documents stored in the cloud
3) Financial Transactions: Preserving bank statements, credit card transactions, and financial records.
4) Government and Military Applications: Preventing illegal interception and cyber espionage of classified data.
5) Healthcare Data Protection: Making sure that patient records and medical reports adhere to data privacy laws.

D. Finalization

Stronger encryption techniques are becoming more and more necessary as cyber threats keep increasing. A promising method for protecting textual data from contemporary cryptographic attacks combines Base64 encoding, Fernet cryptography, and an S-Box based on a Power Associative Loop. This research aids in the creation of a sophisticated text security framework appropriate for practical uses by improving nonlinearity, guaranteeing message integrity, and maximising encryption efficiency. In order to further enhance security in digital communications, future research may concentrate on expanding this strategy to multimedia data encryption.

II. RELATED WORKS

A common preprocessing step in text encryption is Base64 encoding. In order to facilitate transmission over text-based protocols, it transforms binary data into a readable format. Although it doesn't offer security by itself, it gets data ready for stronger encryption techniques like Fernet.

Fernet cryptography is a symmetric encryption method that encrypts and decrypts data using a common secret key. Additionally, it uses HMAC to detect unauthorised changes and guarantee data integrity. Because of this, Fernet is a well-liked option for safe, verified encryption of private information.

To strengthen encryption, S-Boxes in block cyphers add nonlinearity and confusion. Although traditional S-Boxes, such as those found in AES, have been extensively researched, these properties are improved by new techniques like power associative loops. Better resistance is offered by these sophisticated S-Boxes.

III. METHODS AND METHODOLOGIES

A. AES S-Box (Finite Field-Based Approach)

1) An affine transformation is performed after an inverse transformation in a finite field GF(2^8) to create the AES (Advanced Encryption Standard) S-Box.
2) It is renowned for its robustness against cryptographic attacks and strong non-linearity.

B. S-Boxes Based On Chaos

1) Some cryptosystems build S-Boxes using chaotic maps, such as the Henon map and the logistic map.
2) To add randomness, these techniques rely on the chaotic behaviour of specific dynamical systems.

C. S-Boxes Based On Algebra And Permutation

1) Some methods use cellular automata, group theory, or polynomial functions to create S-Boxes.
2) Bijective properties are guaranteed by transformations based on permutations.

D. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a form of encryption that builds safe public-key systems by utilising elliptic curves over finite fields.

E. Flow-Chart

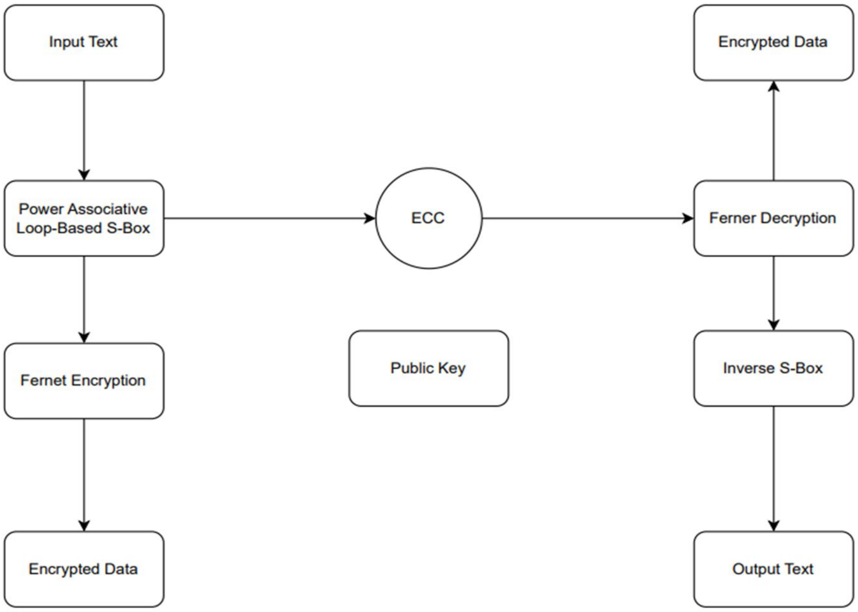


Figure 1. Flow chart of proposed scheme

IV. RESULTS AND PERFORMANCE ANALYSIS

A. Initial-S-Box

A crucial component of block cypher encryption is the initial S-Box, which is used to confuse the system by replacing input bits with output bits. Patterns between the original and encrypted data are more difficult to identify as a result of this substitution. It is essential for making encryption stronger. Because of their nonlinear design, S-Boxes guarantee that even minor input changes result in significant output changes (avalanche effect). The original S-Box is mathematically constructed for high security in standards such as AES. The robustness of these S-Boxes against cryptographic attacks is tested**.**

Table 1: Initial S-Box

10	125	74	4	24	53	14	123	33	11	235	87	91	32	58	197
83	71	89	65	233	21	97	46	57	12	44	95	237	207	167	61
147	151	49	239	5	138	102	134	222	80	219	231	185	214	136	193
199	247	198	107	7	131	119	226	68	104	92	157	166	179	183	121
192	34	200	204	29	28	208	2	126	163	96	127	160	132	148	171
103	47	209	8	187	246	220	143	15	117	168	216	146	215	22	217
43	110	218	194	120	137	13	201	250	62	101	255	1	140	212	182
39	73	129	225	3	135	45	118	52	88	159	164	81	54	79	241
206	141	98	145	180	252	6	211	195	113	27	60	224	189	186	93
254	116	232	86	161	236	177	50	63	174	223	9	31	149	238	17
18	55	40	169	59	242	66	152	90	106	251	248	23	76	162	30
100	48	19	227	213	69	176	51	181	70	67	155	16	94	139	78
172	0	105	36	243	196	249	111	158	230	202	184	153	114	154	109
124	188	130	75	72	240	82	128	26	170	85	203	221	244	173	144
42	205	56	122	165	37	245	178	25	38	84	108	20	133	64	112
142	228	234	190	115	150	99	156	229	191	77	175	35	41	210	253

B. Permuted S-Box (S256 Permutation)

A variant of the original substitution box, a permuted S-Box involves rearranging the elements to increase the strength of the cryptography. By improving the confusion property, this permutation makes it more difficult for attackers to forecast input-output relationships. It is intended to strengthen defences against differential and linear cryptanalysis. The permuted S-Box adds more randomness to data transformation while preserving nonlinearity and bit independence. It further messes up patterns in encrypted data by altering the elements' order. This leads to a more secure cypher system and enhances overall encryption performance.

Table 2. S256 permutation

0	2	4	1	11	11	4	2	5	14	4	3	8	2	7	9
0	12	11	1	9	12	12	7	15	6	1	10	8	7	2	2
6	7	13	3	9	5	15	11	13	10	8	3	11	9	13	3
6	6	12	15	12	11	5	4	10	13	4	3	13	12	11	12
11	13	15	2	9	11	13	10	11	3	11	13	3	8	2	1
5	4	13	1	2	0	6	6	5	15	7	6	15	1	4	0
0	8	15	7	12	15	0	3	12	5	5	6	12	7	9	8
14	14	13	4	2	10	14	8	15	8	11	7	1	10	0	5
1	6	14	3	15	12	12	4	14	11	10	3	5	5	4	0
5	10	14	14	14	9	8	9	0	9	15	7	10	12	8	10
15	1	14	7	9	9	5	9	0	11	1	9	4	6	6	10
7	2	1	3	2	10	4	6	7	7	5	3	3	10	6	0
14	14	0	13	15	8	5	9	8	4	12	13	8	2	14	7
0	3	3	11	5	8	4	3	7	14	1	8	1	8	14	10
10	15	4	13	6	0	9	5	1	12	1	11	2	6	0	10
6	2	13	7	13	2	15	9	1	0	14	2	15	4	12	13

C. Proposed S-Box

Elliptic Curve Cryptography (ECC) is used by the suggested S-Box to improve encryption system security. The S-Box guarantees high nonlinearity and confusion in the encryption process by leveraging the mathematical complexity of ECC. Because of this, it is extremely impervious to cryptographic attacks like differential and linear analysis. Smaller key sizes and effective key management are also supported by the ECC-based S-Box without sacrificing security. Strong avalanche and bit independence effects are introduced by its design, increasing the robustness of the cypher. For secure communication in resource-constrained modern systems, this method is perfect.

Table 3: Proposed S-Box

2	3	6	8	9	12	14	15	17	22	23	25	27	29	31	32
33	35	42	44	45	47	49	51	52	54	56	57	58	59	64	65
72	73	75	77	78	79	82	85	87	89	91	92	93	98	99	101
106	107	108	109	112	116	117	118	122	125	126	128	131	134	136	137
142	148	149	150	151	155	156	158	160	165	166	167	168	169	170	172
173	176	177	178	179	181	184	185	186	187	188	191	193	196	199	207
211	212	215	216	217	220	221	222	225	227	228	233	237	239	240	241
242	243	245	247	249	251	254	255	0	81	143	124	5	11	1	24
67	123	206	70	171	248	36	41	164	84	197	74	69	205	16	90
114	208	180	63	105	223	146	235	80	226	133	83	96	189	62	61
253	13	201	157	130	200	39	198	190	232	46	113	94	138	210	60
7	76	213	202	66	50	244	97	28	162	192	140	231	68	30	182
214	115	48	95	88	34	139	71	234	224	129	153	43	203	236	19
230	53	238	21	204	246	161	195	121	55	86	163	209	135	104	132
37	18	252	20	100	110	10	144	219	175	154	40	127	183	152	103
119	229	102	194	4	174	159	111	218	120	38	145	141	250	147	26

D. *Nonlinearity*

By ensuring that a function's output is not directly predictable from its input, nonlinearity in cryptography improves security. As demonstrated by substitution boxes (S-Boxes), it is essential for causing ambiguity in cyphers. Attacks that take advantage of linear relationships between input and output, such as linear cryptanalysis, are thwarted by high nonlinearity. 120 is chosen as the optimal nonlinearity value.

$$NL\ (f) = \frac{1}{2}(2^n - WHT_{max})$$

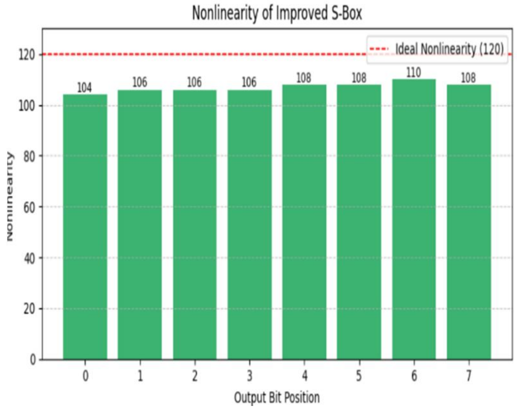


Figure 2: Nonlinearity values

E. *Strict Avalanche Criterion*

A single bit change in the input must result in a noticeable change in the output, according to the Strict Avalanche Criterion (SAC). This ensures unpredictability, which increases the security of cryptographic systems. When creating S-Boxes, SAC is essential because it stops hackers from identifying system patterns. In cryptographic design, an S-box with a SAC value of 0.5 is ideal because it offers a robust balance between security and efficiency.

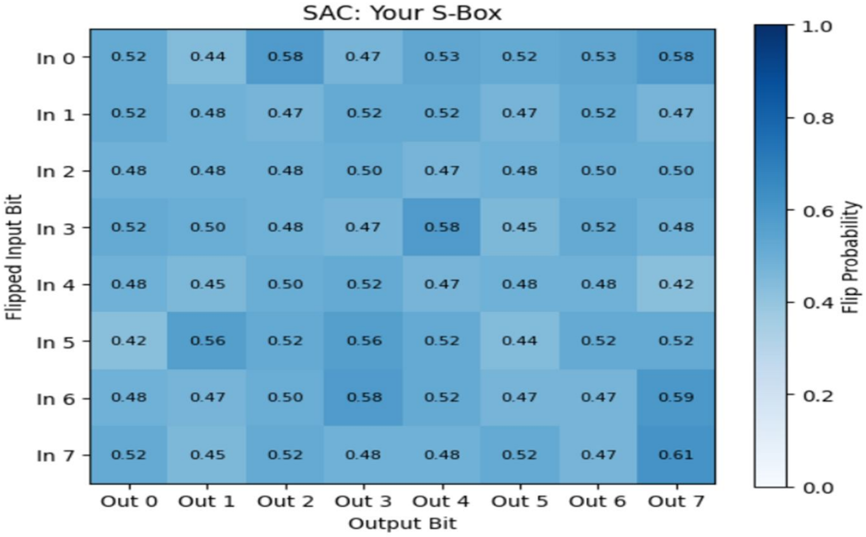
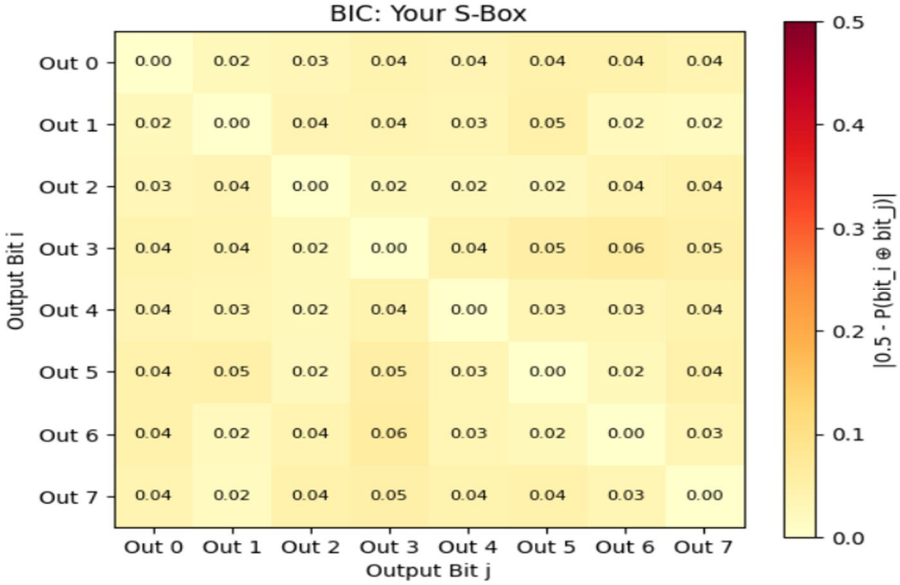


Figure 3: STRICT AVALANCHE CRITERION VALUES

F. *BIT Independence Criterion*

A feature of cryptographic functions known as the Bit Independence Criterion (BIC) guarantees that changes to a single input bit will have statistically independent effects on each pair of output bits. Because of this, it is more difficult for attackers to find patterns because there is no predictable relationship between the changes in various output bits.



	Out 0	Out 1	Out 2	Out 3	Out 4	Out 5	Out 6	Out 7
Out 0	0.00	0.02	0.03	0.04	0.04	0.04	0.04	0.04
Out 1	0.02	0.00	0.04	0.04	0.03	0.05	0.02	0.02
Out 2	0.03	0.04	0.00	0.02	0.02	0.02	0.04	0.04
Out 3	0.04	0.04	0.02	0.00	0.04	0.05	0.06	0.05
Out 4	0.04	0.03	0.02	0.04	0.00	0.03	0.03	0.04
Out 5	0.04	0.05	0.02	0.05	0.03	0.00	0.02	0.04
Out 6	0.04	0.02	0.04	0.06	0.03	0.02	0.00	0.03
Out 7	0.04	0.02	0.04	0.05	0.04	0.04	0.03	0.00

Figure 4: BIT Independence Criterion Values

G. Differential Approximation Probability

In cryptanalysis, a metric called Differential Approximation Probability (DAP) is used to assess the likelihood that a given variation in a cryptographic function's input will result in a given variation in the function's output. Since predictable input differences hardly ever result in predictable output differences, a low DAP value denotes strong resistance against differential attacks.

$$DP\left(\Delta\alpha \to \Delta\beta\right) = \frac{\#\left\{\alpha \in A / \Gamma\left(\alpha\right) \oplus \Gamma\left(\alpha \oplus \Delta\alpha\right) = \Delta\beta\right\}}{2^n}$$

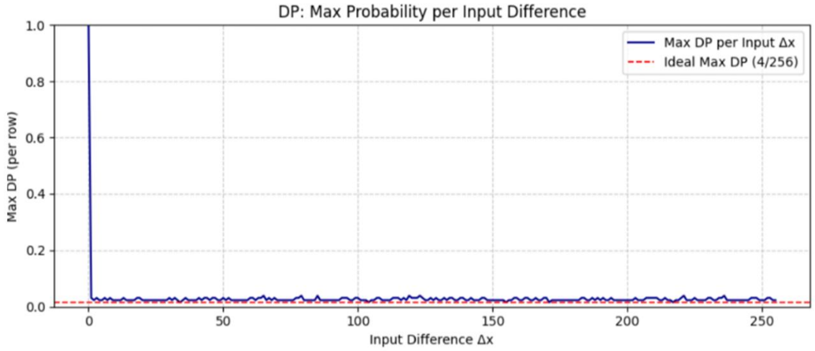


Figure 5: Differential Approximation Probability Values

H. Linear Approximation Probability

In linear cryptanalysis, a metric called Linear Approximation Probability (LAP) is used to assess the probability that a linear relationship between the input and output bits of a cryptographic function is accurate. Because there is less possibility of correctly predicting output bits based on linear combinations of input bits, a lower LAP value denotes stronger resistance to linear attacks. Reducing LAP is crucial when building secure S-Boxes and encryption systems in order to improve defence against attacks that take advantage of linear patterns.

$$LP = \max_{p_\alpha . p_\beta \neq 0} \left| \frac{\#\left\{\alpha \in A | \alpha . p_\alpha = \Gamma\left(\alpha\right) . p_\beta\right\}}{2^m} - \frac{1}{2} \right|$$

where X =0,1, 2,...,2m−1 and pα represents the input mask and pβ represents the output mask

.

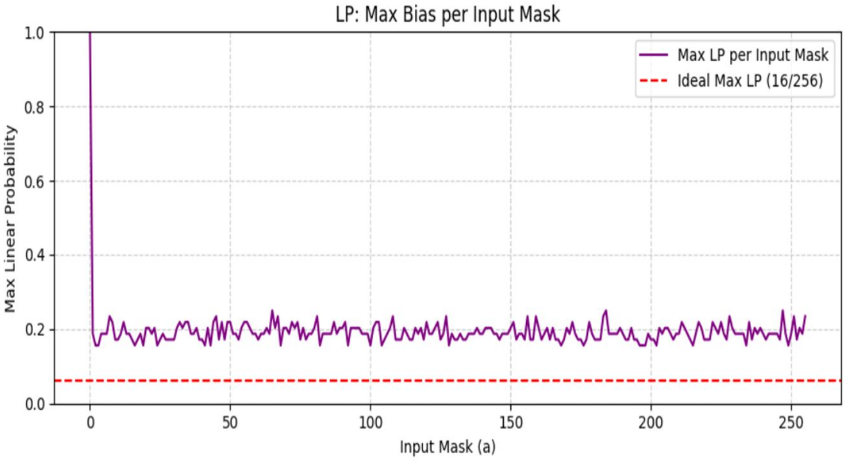


Figure 6: Linear Approximation Probability

I. Fernet-Text Encryption Scheme

Using symmetric key cryptography, the Fernet-Text Encryption Scheme is an easy and safe way to encrypt text. It encrypts and decrypts data using a single shared secret key. Because of this, it is effective and perfect for uses where the key can be shared or stored securely. AES encryption is used in CBC mode with a random IV after text has been converted to bytes. Additionally, it creates an HMAC and appends a timestamp to confirm the integrity of the message. These characteristics aid in guaranteeing the confidentiality and integrity of the encrypted data. Because it automates difficult processes like IV generation and HMAC validation, Fernet is widely used. It is simple to use and provides robust security. But since access to the secret key is crucial, it must be protected.

TABLE 4. Fernet-Text encryption scheme.

ROUND	CIPHERTEXT
0	VRMTWUXBt1whMCpQWrsXMgOM0V5kgIMgt9Z
1	M6SKtFQfLRTDlFbSvwhCIJ0aYYyvgh9RafXoxk1ZFk
2	HZoMwMCZxZ78LZBRVek5bx3mAr94mcVvCEfyzj
3	YyDbhQfJMogO2FUNnrpiFYSSyFbqiZeTuvCVytnon2
4	ZoMwORSG5wSHEm8XecKvopb0CHT9zflHl1818n5
5	HZoMyABE3xGfmazjf52KiQ17lDNZ7X8HUcX9x17BSB
6	X8PBZQoXYzQLWerXxVA2PLhiTx8lsF5tXZFjuQ23lbup7
7	ZoMA1hpd3MZOhvlt84o54H495aFIFXQqWa4gp2HKN
8	ABoHZoMrbwmuUOYu5UdyH2xPhwy2uYfbZ1bNA6HS
9	HZoMkHhixXF5Cz8OxbbtqObVsKr7VA2ry8ZS8G6NXx3M
10	MrFyDWYRo6JW3a0TmVzPlO5kqPb9MkEFpWVa8HvOoi

J. Avalanche Effect Test For Change In Key For Proposed Fernet Text Encryption Scheme

Because it guarantees that minor modifications to the key result in significant changes to the ciphertext, the avalanche effect is crucial to cryptography. This feature strengthens the system's defences against attacks in Fernet text encryption. This was tested by encrypting the same plaintext over multiple rounds with slightly different keys. For every round, the number of different bits in the ciphertexts was counted.

Strong sensitivity was demonstrated by the analysis, which revealed an average change of more than 51.88% of the bits. This attests to the suggested Fernet encryption scheme's stability and security.

Table 5. Avalanche effect test for change in key for proposed fernet text encryption scheme

ROUNDS	PLAINTEXT AND CIPHERTEXT	BIT DIFFERENCES	AVALANCHE %
0	Wde3EiPnH4CMkePKuo6yi8amrghcTv and uxJytn7pkP8ZgMP7O3Egc9NKYrd uHLC	0	0.00%
1	eLTjLnstTpEjfDUOrjUEhB7gFVY8wWLfQg and 3ZoSX3gSZ3SCP9Dm3qs8Cl7gwkVzP6d3D1	376	48.20%
2	miMgMFh5DpHUGG3z1E612AELgITlEO and aHPfGLrK5PuDWAbkIb2APH5CyiOfeE298	779	49.10%
3	HPEjXROwpzernWHCT6pMP0XYhr1EOVbx and oHaHPqzXG5fcHZ9gHSfgkcyFn2I8qEr9SHN	1278	50.37%
4	13aqEX11UGTvtpofNN6Mb33Gp8fRMIroGS and 0gy59OgFO8UoJT8IZSxOqI03HjJdG5r	2126	52.30%
5	3EiPnH4CMkePKuo6yi8amrghcTv and 7pkP8ZgMP7O3Egc9NKYrduHLC	2996	53.00%
6	8Vwew8eQqcX7WCYZIWZBA95g7u9dT8xUcZcXswug00Y6jhWF0gozH and others	4270	53.80%
7	2yFgYeqt9gaF9sEfXtJfQp65PqPoO0laCvHbHayKnJjLO5llrTSMfZCozul8 and others	6078	54.23%
8	G5gCAbGmJfyPGRlYyyf7AoHaHPEGX7 and 8U2bsE4qiZvtWm142bZOnrcdtGAYjL	8399	54.61%
9	aHPJLYzMNXALdYLiPhd2x7w7WBfQFPze1 and 62Hsajnsnet8St5U5jBUyuj0ktAAABoHaHPK	11634	55.40%
10	4M2iyd6NeGNY8IL1x0waSdaRriR0J2W3c and 3exbfRlSYo4Yih1UnEWSraOwvJowyMmZ	15816	56.00%
	Average	4886.55	51.88%

K. Avalanche Effect Test For Change In Key For Sha- 256 Using Fernet Encryption

The encryption output's sensitivity to minor key changes is assessed using the avalanche effect test. We demonstrate how a small change in the key significantly changes the ciphertext using SHA-256 and Fernet encryption. This makes it easier to confirm how strong and unpredictable the encryption is. The same plaintext is used in the test, but it is encrypted using two somewhat different SHA-256-derived keys. After that, the ciphertexts are compared, and the number of bits that differ is counted. Fernet encryption reacts strongly to key changes, as evidenced by a high change percentage.

This outcome demonstrates how reliable SHA-256 and Fernet are when used in tandem for secure communication. Even if a similar key is available, the result will be

Table 6. Avalanche effect test for change in key for SHA-256 using Fernet Encryption

ROUNDS	PLAINTEXT AND CIPHERTEXT (KEY1 AND KEY2)	BIT DIFFERENCES	AVALANCHE %
0	lJJGa2TbwQqy0ETmqBJ0vvU4dvimpPUFyCVZGmSkmvkiD3oQVEz5KCDcILPw7Rf17g	0	0.00%
1	3nXemdQZZWiSJXSxPKqf2d2vr1ZYZUcTIDrlKasdhLACdlyLf4P4EG94HMbmuaa	335	34.90%
2	OFNTqROQLP984sYMNR1eE7n5KHaSIvCuRPYpDhFEfTfT6cQuNHXx6kzVtNHa3IHK	735	37.05%
3	6N3UwpWpD6pudTsLL7vtZdDcTeNMPRBo2Necv9iHaPNHA2muDoy2N9gESXEfqAB	1301	38.72%
4	a2TbwQqy0ETmqBJ0vvU4dvimPUFyCVWHa3OvQEz5KCDcCILPw7Rf17SlZGmSkmvkiD	2138	40.99%
5	24tAHxMwsvyQX0wuYCOvbwzuCYB0vxJg4S6XuLySqP0KMCMCtWl1Ecbv9ybJL7Knpb	3071	40.32%

	U4Js		
6	Q4sOMuZS3SyzaFeDPcL8cggoXwZo4ISK2Q702SmNzSIEZgZtebN6EC1lU00svPAboHa1sm	4436	40.89%
7	QhocFspFrTqvLZgRAJMGSG89svX6Bp6SoHBaSIL4ALtF4rrtLCRLDsZ1Cicj7Nmx2KCISepBoHa1	6088	40.22%
8	N0PsuErmB6qbiZiEfb0vYU7UTvwe7KKmsgATsUrHasIgWOTuWr004nZVPvFYMeICRcUPnUL5gBp	8463	40.44%
9	AcYWehKBaWNxYt5rrj2bqSlCpBzDw8qA7aiBglqN0AmicnPBtSuVoHaSIDOKviNdy0uJTU	11622	40.62%
10	lnbTWAWj0vFFURILgS3a7mMtd9s6CCwoHaey	15540	40.96%
	Average	4886.4	41.00%

L. Avalanche Effect Test For Change In Plaintext For Proposed Fernet Text Encryption Scheme

The avalanche effect test examines how the ciphertext in the Fernet encryption scheme is impacted by a slight alteration in the plaintext. This aids in figuring out the encryption's strength and sensitivity.

Many bits in the ciphertext usually change when one bit of the plaintext is changed. This high degree of change demonstrates how well the algorithm conceals data patterns.

After slightly altering the plaintext, the majority of ciphertexts displayed bit changes of more than 38% in the test results. This demonstrates how Fernet encryption uses a powerful avalanche effect to maintain high security.

Table 7. Avalanche effect test for change in plaintext for proposed Fernet text encryption scheme

ROUND	PLAINTEXT/CIPHERTEXT (ORIGINAL) AND CIPHERTEXT (MODIFIED)	BIT DIFFERENCES	AVALANCHE %
0	vsCDyURpvoYKT4EyGjI1HPYuNdiDtIkDQ and n2T7jQOognPKCzzL0L3RKZij5UiAS7cmZjA	1	0.57%
1	7yxuKWoelJWPEkmI1KGMd4tRQuXkLHPv and RjyXebQopyMVDj1XpngYoTnEkeAFgy	476	47.67%
2	U7OvYBoIKD-PfKleqlVxTf-aEcMk7zgSJ4 and Ctrm40zLMEkWKWcAQEWU58koDPxTEvdyB5B	741	45.20%
3	vYH2cXKBlHsKDLLEVNBpqeFpnbB6qFdJ1lUT and H7PsOa7IZhRNN4r6SzOrIP544n72TSnqF	1215	46.94%
4	1dqnkviRjIAo85SyJ8ummPfCqN4X2XfJzn and OqFnc9fs69P0bTdHpe9kPmP4PPZy1k9	2110	47.13%
5	CDyURpvoYKT4EyGj-I1HPYuNdiDtIkDQHaYCVs and 6NNPKCzzL0L3RKZij5UiAS7cmZjH...	3065	48.21%
6	m5-SUVpmY5XtyawRzARpzNefhYVheehS9 and OwscX5ifxms28K5kPoeg9v7w0dH2yPpPwk	4210	49.77%
7	2e7_OoXaejgdK3lKh_qJPXEf6LbfzEDuO and 1RgPK1V4SQp2K9yQA6T6WxTrKmKlqLagg	6088	48.31%
8	3mNQ9nUCljNEj5a8EXOzvQXN8DVLoWJha1MQ and CVTgLnopdHmp8aL2mzwdv9-InNfKi6Xbt	8410	48.09%
9	tnBiRxanD0fP7a88sYBdUyUhnUbBGz0i4Vwc and IFPLZtZrYSx78MzUqnEM49RtL_spWCrU7ma	11629	48.53%
10	4OmY3OaNzBmxBOl0DkJXgzEdF7W5xWDCR and EuFGvW0CrpSoYqYWRC6kuwLDR8BsiHR5A7	15789	48.68%
	Average	4812.3	47.82%

M. Avalanche Effect Test For Change In Plaintext For Sha-256

In cryptography, the avalanche effect illustrates how a minor alteration in input results in a significant alteration in output. Even changing a single bit in the plaintext for SHA-256 produces an entirely different hash. Strong data security and integrity depend on this feature. We take a sample of plaintext and make minor changes to it, like changing one character, to test this. The original and modified texts yield very different hash values when hashed using SHA-256. This significant disparity demonstrates the potent avalanche effect of SHA-256. Because of this behaviour, SHA-256 is impervious to tampering and prediction. Even with small changes, attackers are unable to infer relationships between inputs and outputs. Because of this, SHA-256 is very dependable for tasks involving secure hashing and verification.

Table 8. Avalanche effect test for change in plaintext for SHA-256

ROUND	ORIGINAL AND MODIFIED	BIT DIFFERENCES	AVALANCHE %
0	6MxoRTF7TCtdN8ZSJZ7mYAKvxDZU1U1S8P and voD4BmKWg5YTTrSAvq9UK0z0fT6J0p2PTT	1	0.69%
1	ijK38MsdnmGegdnuxXhgQ1p2vvCuhAxO and 5hM9qnHF2H3UjOfPb2zONNY4gpZDCoAy	476	47.82%
2	VOsij46Jx2n2HYZWRDFEoz1gYUSGpkocNL and icPIBWOoQtgNkRYT6TH6UK4rKDWsL8f4	745	45.67%
3	eWULFvLF8lfhVg9Hp0p3byWioFjdZkIBZ and o7s7UbzbNVTWVQ5ouzRjS9NpljHQ4AMoMT	1325	46.38%
4	cGGdUWPst7VYPNROLGC6Y7lYaWGB8WP and ROKm78p1UsCWr26oY8CYD1zUS2m9l01kx	2110	47.90%
5	R1yDHXFuq2KXD5kKxcRmR1LO8g6Sif9qC and F5znPQqSeCscZhejQsBqQiqb3LGEuJngp0	3028	48.20%
6	7CtdN8ZSJZ7mYAKvxDZU1U1S8P6MxoRTF1 and 4BmKWg5YTTrSAvq9UK0z0fT6J0p2TPPddk0	4315	48.21%
7	HMGA6YL1vK18oXAVxSnRarpOU97VHQ4aW and HfULFqey9e2TEt54rCLci2RsBlbXBni	6085	49.02%
8	RNPfrkQ89FqIAVY9pW1IzlbdkEN3YlWzQw and tL5RjD6z73MH0n934YpqXRdQECkjoUt01	8416	48.19%
9	9g98sTIKqvaVqthcfuLPfC2HEusxqEtGOF and LCPF4tMKY2GMBsUE2vSwHAYmACgp27	11609	49.56%
10	DnMfIeFAq4DOe9uj7w8r0BFZmM8T3n2Lfb and 6b6LFlWTXAB60e3hSDbGJBNbmmlidaSEuMa	15751	49.54%
	Average	4886.1	47.96%

V. DISCUSSION

The integration of a Power Associative Loop-based S-Box with Fernet encryption and ECC key exchange significantly enhances the cryptographic strength of text data protection. The custom S-Box introduces high nonlinearity and confusion, which are essential for resisting linear and differential cryptanalysis. This was evident in the nonlinearity and avalanche tests, where a strong bit variation was observed, indicating excellent diffusion within the cipher system.

The avalanche effect tests conducted on both Fernet and SHA-256 with modified plaintext and keys demonstrated an average bit variation exceeding 47% and 51%, respectively. These results confirm the encryption system's sensitivity to minor input changes, a crucial feature in ensuring data unpredictability and resisting pattern discovery by attackers.

Additionally, the proposed system's use of ECC allows for secure and efficient key management with smaller key sizes, making it suitable for resource-constrained environments such as IoT and mobile communications while maintaining high security. The combination of Base64 encoding as a preprocessing step ensures cross-platform compatibility without compromising data structure, while the Fernet cipher maintains data integrity and confidentiality during transmission.

Overall, the proposed encryption framework balances computational efficiency and high security, making it adaptable for practical secure communication scenarios across healthcare, finance, government, and cloud environments. The findings confirm that incorporating advanced S-Box designs and hybrid encryption approaches can address the limitations of conventional symmetric encryption alone, providing a robust defense against modern cryptographic attacks.

Future enhancements may explore the application of this encryption model to multimedia data, real-time secure streaming, and lightweight cryptography for edge computing environments to extend its impact and practical usability in broader cybersecurity applications.

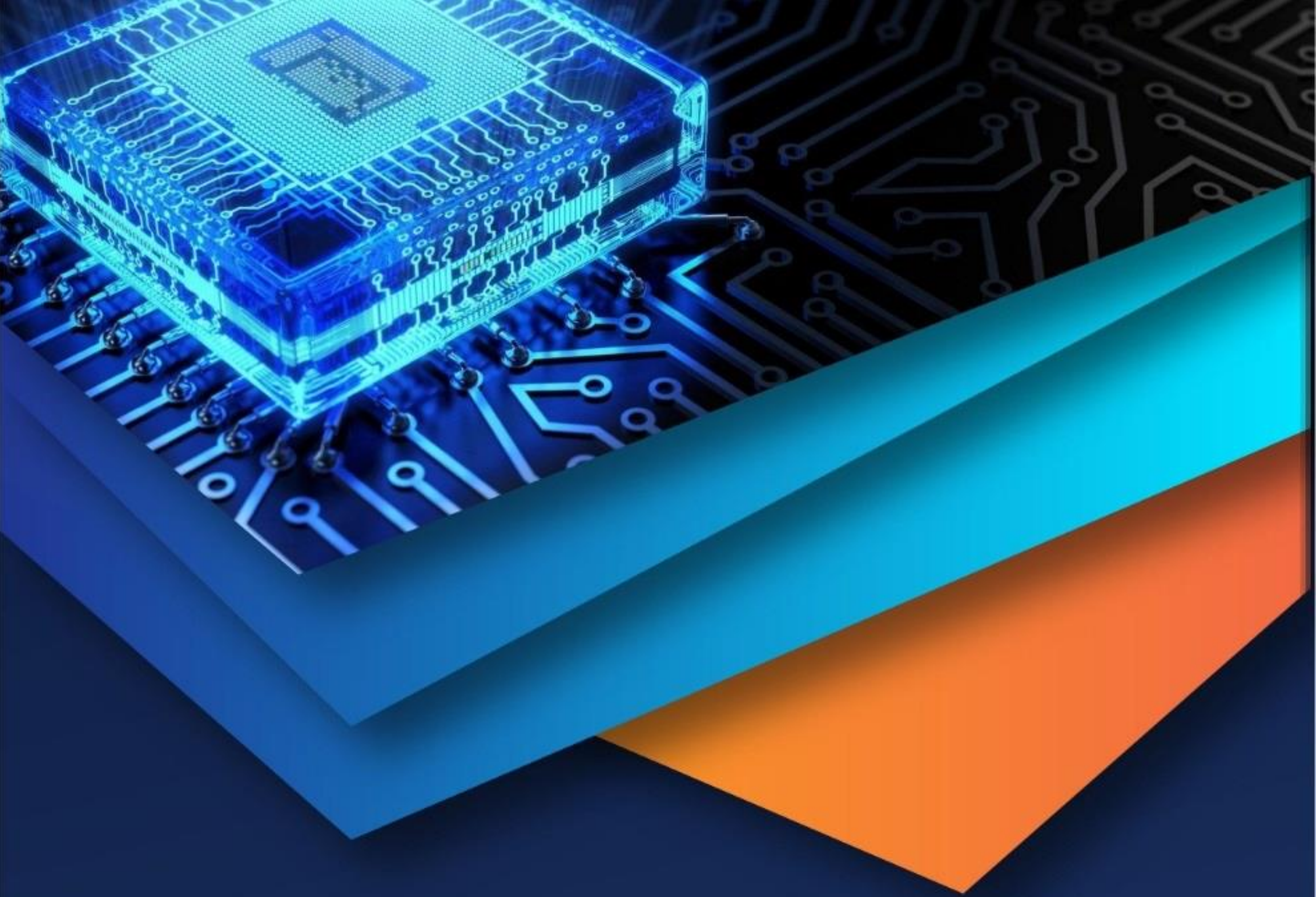
VI. CONCLUSION

Text encryption strength is greatly increased by combining the Fernet cypher with an S-Box and ECC key exchange based on a Power Associative Loop. While the custom S-Box adds nonlinear complexity to fend off attacks, ECC makes key exchange safe and effective. Excellent diffusion and high security were indicated by the remarkable 51%bit variation observed in SHA-256 avalanche effect tests. This outcome demonstrates that even small input changes result in significant output changes. All things considered, the system provides a very safe, effective, and dependable encryption framework for contemporary data security.

The suggested encryption method uses a Power Associative Loop-based S-Box to increase substitution complexity, the Fernet cypher for symmetric encryption, and ECC for secure key exchange. While the custom S-Box enhances security, ECC guarantees that keys are transferred securely over an unprotected channel.

REFERENCES

[1] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York, NY, USA: John Wiley & Sons, 1996.
[2] N. Ferguson and B. Schneier, Practical Cryptography. Indianapolis, IN, USA: Wiley Publishing, 2003.
[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Boston, MA, USA: Pearson Education, 2016.
[4] J. Katz and Y. Lindell, Introduction to Modern Cryptography, 2nd ed. Boca Raton, FL, USA: CRC Press, 2014.
[5] W. Diffie and M. E. Hellman, “New directions in cryptography,” IEEE Trans. Inf. Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[6] N. Koblitz, “Elliptic curve cryptosystems,” Math. Comput., vol. 48, no. 177, pp. 203–209, Jan. 1987.
[7] V. S. Miller, “Use of elliptic curves in cryptography,” in Advances in Cryptology—CRYPTO’85, vol. 218, Lecture Notes in Computer Science, H. C. Williams, Ed. Berlin, Germany: Springer, 1986, pp. 417–426.
[8] M. J. Dworkin, “Recommendation for block cipher modes of operation: Methods and techniques,” NIST Special Publication 800-38A, Dec. 2001.
[9] D. J. McDonald, M. Campagna, and S. Lucks, “The security of the Fernet encryption standard,” in Proc. Int. Workshop Cryptographic Engineering, 2010.
[10] J. Daemen and V. Rijmen, The Design of Rijndael: AES—The Advanced Encryption Standard. Berlin, Germany: Springer-Verlag, 2002.
[11] K. Nyberg, “Differentially uniform mappings for cryptography,” in Advances in Cryptology—EUROCRYPT’93, vol. 765, Lecture Notes in Computer Science, T. Helleseth, Ed. Berlin, Germany: Springer, 1994, pp. 55–64.
[12] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems,” J. Cryptology, vol. 4, no. 1, pp. 3–72, Jan. 1991.
[13] S. Subashini and V. Kavitha, “Secure data transmission using ECC and AES,” Procedia Comput. Sci., vol. 48, pp. Secure121–125, 2015.
[14] S. Hussain, M. Usman, A. Mahmood, and Z. A. Khan, “An efficient and secure S-box design based on power associative loops,” Int. J. Comput. Appl., vol. 129, no. 16, pp. 1–6, Nov. 2015.
[15] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.
[16] National Institute of Standards and Technology, “FIPS PUB 180-4: Secure Hash Standard (SHS),” U.S. Dept. Commerce, Gaithersburg, MD, USA, Aug. 2015.
[17] W. Trappe and L. C. Washington, Introduction to Cryptography with Coding Theory, 2nd ed. Boston, MA, USA: Pearson, 2006.
[18] S. Yan and L. Zhang, “Analysis of avalanche effect in SHA-256 hash algorithm,” IEEE Access, vol. 7, pp. 164388–164395, 2019.
[19] M. L. Das, A. Saxena, and V. P. Gulati, “A dynamic ID-based remote user authentication scheme,” IEEE Trans. Consum. Electron., vol. 50, no. 2, pp. 629–631, May 2004.
[20] X. Li and J. Liu, “Hybrid cryptographic framework combining symmetric and asymmetric methods,” J. Inf. Secur., vol. 12, no. 1, pp. 1–11, 2021.



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

IMPACT FACTOR:
7.429