Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/taut20

Homomorphism on bipolar-valued fuzzy sub-bigroup of a bigroup for secured data transmission over WSN

Sheena K. P. & K. Uma Devi

To cite this article: Sheena K. P. & K. Uma Devi (2023) Homomorphism on bipolar-valued fuzzy sub-bigroup of a bigroup for secured data transmission over WSN, Automatika, 64:4, 956-963, DOI: 10.1080/00051144.2023.2226945

To link to this article: https://doi.org/10.1080/00051144.2023.2226945

Published online: 27 Jul 2023.

AUTOMATIKA
2023, VOL. 64, NO. 4, 956–963
https://doi.org/10.1080/00051144.2023.2226945

Homomorphism on bipolar-valued fuzzy sub-bigroup of a bigroup for secured data transmission over WSN

K. P. Sheena[a,b] and K. Uma Devi[a]

[a]Department of Mathematics, Noorul Islam Centre for Higher Education, Kumaracoil, India; [b]Department of Mathematics, Mahatma Gandhi Government Arts College, Mahe, India

ABSTRACT
Cryptography field, which enables secure communication between civilians, governmental organizations, military forces, and many more, addresses security, confidentiality, and integrity of information being conveyed regardless of the medium used. Protection of priceless information resources on intranets, the Internet, and the cloud has become a vital demand of contemporary electronic security systems. In this paper, we deploy homomorphic data encryption (HDE) technique on Bipolar-valued Fuzzy Sub-Bigroups (BVFSB). Intuitionistic Fuzzy Sets were presented by Atanassov in 1986, as a modification of Fuzzy Sets, by taking into consideration the grade of membership value and non-membership value for each element in the universe. A fuzzy algebraic structure known as Bipolar-valued Fuzzy sub-bigroup of a bigroup has been established by applying the concept of bipolar-valued Fuzzy sets to bigroups. Some of the theorems related to homomorphism and anti-homomorphism, are stated and proved.

ARTICLE HISTORY
Received 27 April 2023
Accepted 13 June 2023

KEYWORDS
Bipolar-valued fuzzy set; bipolar-valued fuzzy-subgroup; bigroup; bipolar-valued fuzzy sub-bigroup; bipolar-valued fuzzy normal sub-bigroup; generalized characteristic bipolar-valued fuzzy sub-bigroup

I Introduction

The cyber-physical systems are used frequently in several applications like smart home systems, equipment diagnostics during production, security systems, health care, military applications, etc. The development of IT technology is accelerating over time. Often, wireless sensor networks serve as the systems' obvious base. Sensor networks are wireless networks made up of multiple tiny sensors that are dispersed throughout space. Because wireless sensor networks cannot be protected using standard computer network security measures, unique security measures that are appropriate for sensor networks must be developed. One such measure is the use of homomorphic encryption algorithms. Digital communication is now more susceptible than ever to surveillance or hostile interference, such as hacking or eavesdropping. New techniques for secure transmission via unsecure channels are needed to ensure the security of sensitive data in applications including copyright protection, distant military communication, safe storage, authentication, and secure video conferencing. A unique class of cryptosystems called homomorphic cryptosystems keeps track of group operations carried out on the ciphertexts. The homomorphic characteristic of public key cryptosystems has been utilized in a large number of data security protocols, including electronic voting systems, bidding protocols, cashing systems, and asymmetric photo fingerprinting [1].

As an extension of Fuzzy sets [2], in 1994, W.R.Zhang [3,4] introduced 'Bipolar-valued Fuzzy sets' and was further developed by Lee [5,6]. In a bipolar-valued Fuzzy set items with a membership degree of 0 are irrelevant to the corresponding property whereas those with a membership degree of 0 1 and −1 0] partially meet the property and the implicit counter property, respectively. Vasantha kandasamy.W.B [7] introduced the basic idea of fuzzy bigroup. M.S.Anitha et al. [8] introduced the bipolar-valued Fuzzy subgroup and A.Balasubramanian et al. [9] introduced intuitionistic fuzzy sub-bigroup of a bigroup. Justin Prabu.T and K.Arjunan [10] introduced Q-fuzzy subbigroup of a bigroup. In continuation with the works related to Bipolar-valued Fuzzy Sets, Sheena. K. P and K.Uma Devi [11] familiarized bipolar-valued Fuzzy sub-bigroup (^{BVF}SBG) of a bigroup by applying the concept of bipolar-valued Fuzzy sets, on bigroups. Bigroup is an algebraic structure consisting of two groups with respective group operations.

Abdulatif Alabdulati et al. [12] presented the lightweight homomorphic encryption algorithm in privacy-preserving cloud-based practical and secure billing system. The effectiveness, reliability, and adaptability of operating smart infrastructure could be considerably increased if sensors could be integrated with cloud-based data storage and processing. One of the most valuable features of this privacy-preserving

CONTACT K. P. Sheena sheenakp.researchscholar@gmail.com; sheenasneham@yahoo.com Department of Mathematics, Noorul Islam Centre for Higher Education, Kumaracoil, Tamil Nadu, India; Department of Mathematics, Mahatma Gandhi Government Arts College, Mahe, (P O) New Mahe, U T of Puducherry, India

system has the potential for secure transfer of billing management into the cloud, with on-demand data retrieval and statistical analyses. A scrambled image can then be safely obtained by the dealer. In fact, using this method, each player merely needs to deduct their own key image from the scrambled image to extract the secret image.

1.1. Objective

The objectives of this research are as follows:

(1) The extracted shared secret data is extracted once the encryption and decryption processes have been completed in the proposed system.
(2) With the help of the encryption technique known as homomorphic encryption, you can add and multiply cipher texts in order to get this output which match an outcome of similar one.
(3) Encoding messages or information so that only authorized parties can read it is known as encryption in cryptography.
(4) A message or piece of information, known as plaintext in an encryption scheme, is encrypted using an encryption algorithm to create cipher text that can only be decoded and read.
(5) An encryption technique typically employs a pseudo-random encryption key produced by an algorithm for technical reasons.

1. Preliminaries

Definition 1.1 ([8]): Let G be a group. If the following criteria are met, a bipolar-valued Fuzzy subset N of G, with the two membership values, N^{+m} and N^{-m} is said to be a bipolar-valued Fuzzy subgroup of G if, (i) $N^{+m}(ab^{-1}) \geq \min\{N^{+m}(a), N^{+m}(b)\}$, (ii) $N^{-m}(ab^{-1}) \leq \max\{N^{-m}(a), N^{-m}(b)\}$, for all a and b in G.

Definition 1.2 ([11]): Let $(G = G_1 \cup G_2, +, \cdot)$ be a bigroup. If there are two bipolar-valued Fuzzy subsets A_1 of G_1 and A_2 of G_2 such that (i) $A = A_1 \cup A_2$ (ii) A_1 is a bipolar-valued Fuzzy subgroup of $(G_1, +)$ (iii) A_2 is a bipolar-valued Fuzzy subgroup of $(G_2, \cdot)$, then the bipolar-valued Fuzzy set A of G is said to be a bipolar-valued Fuzzy sub-bigroup.

Definition 1.3 ([8]): Let $(G, *)$ be a group. If $N^{+m}(a * b) = N^{+m}(b * a)$, and $N^{-m}(a * b) = N^{-m}(b * a)$ for every a and b in G, then the bipolar-valued Fuzzy subgroup N of G is said to be a bipolar-valued Fuzzy normal subgroup of G.

Definition 1.4: Let $(G = G_1 \cup G_2, +, \cdot)$ be a bigroup. If there are two bipolar-valued Fuzzy subsets A_1 of G_1 and A_2 of G_2 such that, (i) $A = A_1 \cup A_2$ (ii) A_1 is a normal bipolar-valued Fuzzy subgroup of $(G_1, +)$ (iii) A_2 is a normal bipolar-valued Fuzzy subgroup of $(G_2, \cdot)$, then the bipolar-valued Fuzzy subset A of G is said to be a bipolar-valued Fuzzy normal sub-bigroup of G.

Definition 1.5 ([13]): Let $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ be any two bigroups. Then, the function $f : G_1 \to G_2$ is an anti-homomorphism if $f(x + y) = f(y) + f(x)$ for all x and y in H_1 and $f(x \cdot y) = f(y) \cdot f(x)$ for all x and y in F_1.

Definition 1.6 ([13]): Let $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ be two bigroups. Let $f : G_1 \to G_2$ be given as an anti-homomorphism. If f is one-to-one and onto, then f is called an anti-isomorphism.

Theorem 1.7 ([10]): *Let $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ be any two bigroups with identities. If $f : G_1 \to G_2$ is an anti-homomorphism, then $f(0) = 0'$, $f(1) = 1'$ where 0, 1 and $0', 1'$ are identities of G_1 and G_2 respectively. (ii) $f(-a) = -f(a)$ for all $a \in H_1$ and $f(a^{-1}) = (f(a))^{-1}$ for all $a \in F_1$*

Definition 1.8 ([13]): Let $f : X \to X'$ be an onto function defined on X. Let A represent a fuzzy bi-polar subset of X. Then, the image of A under f is indicated by $f(A) = V$, which is a bipolar-valued Fuzzy subset on $f(X) = X'$ and is defined by $V^{+m}(q) = \sup_{p \in f^{-1}(q)} A^{+m}(p)$ and $V^{-m}(q) = \inf_{p \in f^{-1}(q)} A^{-m}(p)$ for all q in X'. Let B be a fuzzy bi-polar valued subset of X'. The pre-image of B which is denoted as $f^{-1}(B) = W$ is defined by $W^{+m}(p) = B^{+m}(f(p))$ and $W^{-m}(p) = B^{-m}(f(p))$ for every p in X.

2. Theorems

Theorem 2.1: *Given two bigroups $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ and an isomorphism f from G_1 to G_2. Then the image of a bipolar-valued Fuzzy sub-bigroup of G_1 under f is a bipolar-valued Fuzzy sub-bigroup of G_2.*

Proof: Let $f : G_1 \to G_2$ be an isomorphism and let $A = M \cup N = (M \cup N)^{+m}, (M \cup N)^{-m}$ be a bipolar valued fuzzy sub-bigroup of G_1.

Then, $f(A) = ((f(M) \cup f(N))^{+m}, (f(M) \cup f(N))^{-m})$, where $(f(M))^{+m}(y) = \sup_{x \in f^{-1}(y)} M^{+m}(x)$; $(f(M))^{-m}(y) = \inf_{x \in f^{-1}(y)} M^{-m}(x)$, for all y in H_2 and $(f(N))^{+m}(y) = \sup_{x \in f^{-1}(y)} N^{+m}(x)$; $(f(N))^{-m}(y) = \inf_{x \in f^{-1}(y)} N^{-m}(x)$, for all y in F_2.

Let $f(a_1)$ and $f(b_1)$ be in G_2. If $f(a_1)$ and $f(b_1)$ are in H_2, then $(f(M))^{+m}(f(a_1) - f(b_1)) = (f(M))^{+m}(f(a_1 - b_1)) = \sup_{x \in f^{-1}(f(a_1 - b_1))} M^{+m}(x) = \sup_{f(x) \in (f(a_1 - b_1))} M^{+m}(x) = M^{+m}(a_1 - b_1) \geq \min$

$\{M^{+m}(a_1), M^{+m}(b_1)\} = \min \{f(M)^{+m}(f(a_1)), f(M)^{+m}(f(b_1))\}$, as $f : G_1 \to G_2$ is an isomorphism. Also $(f(M))^{-m}(f(a_1) - f(b_1)) = (f(M))^{-m}(f(a_1 - b_1)) = \inf_{x \in f^{-1}(f(a_1 - b_1))} M^{-m}(x) = \inf_{f(x) \in (f(a_1 - b_1))} M^{-m}(x) = M^{-m}(a_1 - b_1) \le \max \{M^{-m}(a_1), M^{-m}(b_1)\} \le \max \{f(M)^{-m}(f(a_1)), f(M)^{-m}(f(b_1))\}$.

Similarly, if $f(a_1)$ and $f(b_1)$ are in F_2, then $(f(N))^{+m}(f(a_1)(f(b_1))^{-1}) = (f(N))^{+m}(f(a_1 b_1^{-1}) = \sup_{x \in f^{-1}(f(a_1 b_1^{-1})} N^{+m}(x) = \sup_{f(x) \in (f(a_1 b_1^{-1}))} N^{+m}(x) = N^{+m}(a_1 b_1^{-1}) \ge \min \{N^{+m}(a_1), N^{+m}(b_1)\} = \min \{f(N)^{+m}(f(a_1)), f(N)^{+m}(f(b_1))\}$.

Also, $(f(N))^{-m}(f(a_1)(f(b_1))^{-1}) = (f(N))^{-m}(f(a_1 b_1^{-1}) = \inf_{x \in f^{-1}(f(a_1 b_1^{-1})} N^{-m}(x) = \inf_{f(x) \in (f(a_1 b_1^{-1})} N^{-m}(x) = N^{-m}(a_1 b_1^{-1}) \le \max \{N^{-m}(a_1), N^{-m}(b_1)\} \le \max \{f(N)^{-m}(f(a_1)), f(N)^{-m}(f(b_1))\}$.

Hence $f(A) = ((f(M) \cup f(N))^{+m}, (f(M) \cup f(N))^{-m})$, is a bipolar valued fuzzy sub-bigroup of G_2. ■

Theorem 2.2: *Given two bigroups $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ and a homomorphism, $f : G_1 \to G_2$. Then for a bipolar valued fuzzy sub-bigroup of G_2, its pre-image is a bipolar valued fuzzy sub-bigroup of G_1.*

Proof: Let $f : G_1 \to G_2$ be a homomorphism. Let $B = R \cup S = (R \cup S)^{+m}, (R \cup S)^{-m}$ be a bipolar valued fuzzy sub-bigroup of G_2.

$f^{-1}(B) = f^{-1}(R \cup S) = f^{-1}(R) \cup f^{-1}(S) = (f^{-1}(R) \cup f^{-1}(S))^{+m}, f^{-1}(R) \cup f^{-1}(S))^{-m}$, where $(f^{-1}(R))^{+m}(x) = R^{+m}(f(x)); (f^{-1}(R))^{-m}(x) = R^{-m}(f(x))$ for all x in H_1 and $(f^{-1}(S))^{+m}(x) = S^{+m}(f(x)); (f^{-1}(S))^{-m}(x) = S^{-m}(f(x))$ for all x in F_1.

Let a_1 and b_1 be in G_1. If a_1 and b_1 are in H_1, then $(f^{-1}(R))^{+m}(a_1 - b_1) = R^{+m}(f(a_1 - b_1) = R^{+m}(f(a_1) - f(b_1)) \ge \min\{R^{+m}(f(a_1), R^{+m}(f(b_1)\} \ge \min (f^{-1}(R))^{+m}(a_1), (f^{-1}(R))^{+m}(b_1))$.

Also $(f^{-1}(R))^{-m}(a_1 - b_1) = R^{-m}(f(a_1 - b_1) = R^{-m}(f(a_1) - f(b_1)) \le \max\{R^{-m}(f(a_1), R^{-m}(f(b_1)\} \le \max (f^{-1}(R))^{-m}(a_1), (f^{-1}(R))^{-m}(b_1)$.

Similarly, if a_1 and b_1 are in F_1, then,

$$\begin{aligned}(f^{-1}(S))^{+m}(a_1 b_1^{-1}) &= S^{+m}(f(a_1 b_1^{-1}) \\ &= S^{+m}(f(a_1)(f(b_1))^{-1}) \\ &\ge \min \{S^{+m}(f(a_1), S^{+m}(f(b_1)\} \\ &\ge \min(f^{-1}(S))^{+m}(a_1), (f^{-1}(S))^{+m}(b_1)).\end{aligned}$$

Also $(f^{-1}(S))^{-m}(a_1 b_1^{-1}) = S^{-m}(f(a_1 b_1^{-1}) = S^{-m}(f(a_1)(f(b_1))^{-1}) \le \max \{S^{-m}(f(a_1), S^{-m}(f(b_1)\} = \max\{(f^{-1}(S))^{-m}(a_1), (f^{-1}(S))^{-m}(b_1)\}$

Hence $f^{-1}(B) = f^{-1}(R \cup S) = f^{-1}(R) \cup f^{-1}(S) = (f^{-1}(R) \cup f^{-1}(S))^{+m}, (f^{-1}(R) \cup f^{-1}(S))^{-m}$, is a bipolar valued fuzzy sub-bigroup of G_1. ■

Theorem 2.3: *Let $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ be any two bigroups. Then the anti-isomorphic image of a bipolar valued fuzzy sub-bigroup of G_1 is a bipolar valued fuzzy sub-bigroup of G_2.*

Proof: Let $f : G_1 \to G_2$ be an anti-isomorphism. Let $A = M \cup N = (M \cup N)^{+m}, (M \cup N)^{-m}$ be a bipolar valued fuzzy sub-bigroup of $G_1 = H_1 \cup F_1$. To prove that $f(A) = ((f(M) \cup f(N))^{+m}, (f(M) \cup f(N))^{-m})$, is a bipolar valued fuzzy sub-bigroup of G_2.

Let $f(a_1)$ and $f(b_1)$ be in G_2. If $f(a_1)$ and $f(b_1)$ are in H_2, then

$$\begin{aligned}(f(M))^{+m}&(f(a_1) - f(b_1)) \\ &= (f(M))^{+m}(f(-b_1 + a_1)) \\ &= \sup_{x \in f^{-1}(f(-b_1 + a_1)} M^{+m}(x) \\ &= \sup_{f(x) \in (f(-b_1 + a_1))} M^{+m}(x) = M^{+m}(-b_1 + a_1) \\ &\ge \min\{M^{+m}(a_1),\ M^{+m}(b_1)\} \\ &= \min \{(f(M))^{+m}(f(a_1), (f(M))^{+m}(f(b_1)\}.\end{aligned}$$

Also, $(f(M))^{-m}(f(a_1) - f(b_1)) = (f(M))^{-m}(f(-b_1 + a_1)) = \inf_{x \in f^{-1}(f(-b_1 + a_1)} M^{-m}(x) = \inf_{f(x) \in (f(-b_1 + a_1))} M^{-m}(x) = M^{-m}(-b_1 + a_1) \le \max\{M^{-m}(a_1), M^{-m}(b_1)\} = \max \{f(M)^{-m}(f(a_1), f(M)^{-m}(f(b_1)\}$

If $f(a_1)$ and $f(b_1)$ are in F_2, then $(f(N))^{+m}(f(a_1)(f(b_1))^{-1}) = f(N)^{+m}(f(b_1^{-1} a_1) = \sup_{x \in f^{-1}(f(b_1^{-1} a_1)} N^{+m}(x) = \sup_{f(x) \in (f(b_1^{-1} a_1)} N^{+m}(x) = N^{+m}(b_1^{-1} a_1) \ge \min \{N^{+m}(a_1), N^{+m}(b_1)\} = \min \{f(N)^{+m}(f(a_1)), f(N)^{+m}(f(b_1))\}$.

Also, $(f(N))^{-m}(f(a_1)(f(b_1))^{-1}) = (f(N))^{-m}(f(b_1^{-1} a_1) = \inf_{x \in f^{-1}(f(b_1^{-1} a_1)} N^{-m}(x) = \inf_{f(x) \in (f(b_1^{-1} a_1))} N^{-m}(x) = N^{-m}(b_1^{-1} a_1) \le \max\{N^{-m}(a_1), N^{-m}(b_1)\} \le \max\{f(N)^{-m}(f(a_1)), f(N)^{-m}(f(b_1))\}$

Hence, $f(A) = ((f(M) \cup f(N))^{+m}, (f(M) \cup f(N))^{-m})$, is a bipolar valued fuzzy sub-bigroup of G_2. ■

Theorem 2.4: *Let $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ be any two bigroups. Then the anti-homomorphic preimage of a bipolar valued fuzzy sub-bigroup of G_2 is a bipolar valued fuzzy sub-bigroup of G_1.*

Proof: Let $f : G_1 \to G_2$ be an anti-homomorphism. Let $B = R \cup S = (R \cup S)^{+m}, (R \cup S)^{-m}$ be a bipolar valued fuzzy sub-bigroup of G_2.

Let a_1 and b_1 be in G_1. If a_1 and b_1 are in H_1, then $(f^{-1}(R))^{+m}(a_1 - b_1) = R^{+m}(f(a_1 - b_1) = R^{+m}(f(-b_1) + f(a_1)) = R^{+m}(-f(b_1) + f(a_1)) \ge \min \{R^{+m}(f(a_1), R^{+m}(f(b_1)\} \ge \min (f^{-1}(R))^{+m}(a_1), (f^{-1}(R))^{+m}(b_1))$.

Also $(f^{-1}(R))^{-m}(a_1 - b_1) = R^{-m}(f(a_1 - b_1) = R^{-m}(f(-b_1) + f(a_1)) \le \max\{R^{-m}(f(a_1), R^{-m}(f(b_1)\} \le \max (f^{-1}(R))^{-m}(a_1), (f^{-1}(R))^{-m}(b_1)$.

Similarly, if a_1 and b_1 are in F_1, then,

$$(f^{-1}(S))^{+m}(a_1b_1{}^{-1}) = S^{+m}(f(a_1b_1{}^{-1})$$
$$= S^{+m}((f(b_1))^{-1}f(a_1))$$
$$\geq \min\{S^{+m}(f(a_1), S^{+m}(f(b_1)\}$$
$$\geq \min(f^{-1}(S))^{+m}(a_1), (f^{-1}(S))^{+m}(b_1)).$$

Also $(f^{-1}(S))^{-m}(a_1b_1{}^{-1}) = S^{-m}(f(a_1b_1{}^{-1}) = S^{-m}((f(b_1))^{-1}f(a_1)) \leq \max\{S^{-m}(f(a_1), S^{-m}(f(b_1)\} = \max\{(f^{-1}(S))^{-m}(a_1), (f^{-1}(S))^{-m}(b_1)\}$

Hence $f^{-1}(B) = f^{-1}(R \cup S) == (f^{-1}(R) \cup f^{-1}(S))^{+m}, (f^{-1}(R) \cup f^{-1}(S))^{-m})$, is a bipolar valued fuzzy sub-bigroup of G_1. ■

Theorem 2.5: *Let $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ be any two bigroups. The isomorphic image of a bipolar valued fuzzy normal sub-bigroup of G_1 is a bipolar valued fuzzy normal sub-bigroup of G_2.*

Proof: Let $f : G_1 \to G_2$ be an isomorphism and let $A = M \cup N = (M \cup N)^{+m}, (M \cup N)^{-m}$ be a bipolar valued fuzzy normal sub-bigroup of G_1. To prove that $f(A)$ is a bipolar valued fuzzy normal sub-bigroup of G_2.

By theorem 2.1, $f(A)$ is a bipolar valued fuzzy sub-bigroup of G_2.

Let $f(a_1)$ and $f(b_1)$ be in G_2. If $f(a_1)$ and $f(b_1)$ are in H_2, then

$$f(M)^{+m}(f(a_1) + f(b_1)) = f(M)^{+m}(f(a_1 + b_1))$$
$$= M^{+m}(a_1 + b_1) = M^{+m}(b_1 + a_1)$$
$$= f(M)^{+m}(f(b_1 + a_1)) = f(M)^{+m}(f(b_1) + (f(a_1)$$

Also,$f(M)^{-m}(f(a_1) + f(b_1)) = f(M)^{-m}(f(a_1 + b_1)) = M^{-m}(a_1 + b_1) = M^{-m}(b_1 + a_1) = f(M)^{-m}(f(b_1 + a_1)) = f(M)^{-m}(f(b_1) + f(a_1))$.

If $f(a_1)$ and $f(b_1)$ are in F_2, then $f(N)^{+m}(f(a_1)f(b_1)) = f(N)^{+m}(f(a_1b_1) = N^{+m}(a_1b_1) = N^{+m}(b_1a_1) = f(N)^{+m}(f(b_1a_1) = f(N)^{+m}(f(b_1)f(a_1))$.

Also $f(N)^{-m}(f(a_1)f(b_1)) = f(N)^{-m}(f(a_1b_1) = N^{-m}(a_1b_1) = N^{-m}(b_1a_1) = f(N)^{-m}(f(b_1a_1) = f(N)^{-m}(f(b_1)f(a_1))$.

Hence $f(A)$ is a bipolar valued fuzzy normal sub-bigroup of G_2. ■

Theorem 2.6: *Let $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ be any two bigroups. The homomorphic preimage of a bipolar valued fuzzy normal sub-bigroup of G_2 is a bipolar valued fuzzy normal sub-bigroup of G_1.*

Proof: Let $f : G_1 \to G_2$ be a homomorphism.

Let $B = R \cup S = (R \cup S)^{+m}, (R \cup S)^{-m}$ be a bipolar valued fuzzy sub-bigroup of G_2. Then, by theorem 2.2, its homomorphic preimage $f^{-1}(B) = f^{-1}(R \cup S) = ((f^{-1}(R) \cup f^{-1}(S))^{+m}, (f^{-1}(R) \cup f^{-1}(S))^{-m}))$, is a bipolar valued fuzzy sub-bigroup of G_1.

Let a_1 and b_1 be in G_1. If a_1 and b_1 are in H_1, then $f^{-1}(R)^{+m}(a_1 + b_1) = R^{+m}(f(a_1 + b_1) = R^{+m}(f(a_1) + f(b_1)) = R^{+m}(f(b_1) + f(a_1)) = R^{+m}(f(b_1 + a_1) = f^{-1}(R)^{+m}(b_1 + a_1)$.

Also,$f^{-1}(R)^{-m}(a_1 + b_1) = R^{-m}(f(a_1 + b_1) = R^{-m}((f(a_1 + b_1)) = R^{-m}(f(a_1) + f(b_1)) = R^{-m}(f(b_1) + f(a_1)) = R^{-m}(f(b_1 + a_1) = f^{-1}(R)^{-m}(b_1 + a_1)$.

If a_1 and b_1 are in F_1, then $f^{-1}(S)^{+m}(a_1b_1) = S^{+m}(f(a_1b_1) = S^{+m}(f(a_1)f(b_1)) = S^{+m}(f(b_1)f(a_1)) = S^{+m}(f(b_1a_1) = f^{-1}(S)^{+m}(b_1a_1)$.

Also $f^{-1}(S)^{-m}(a_1b_1) = S^{-m}(f(a_1b_1) = S^{-m}(f(a_1)f(b_1)) = S^{-m}(f(b_1)f(a_1)) = S^{-m}(f(b_1a_1) = f^{-1}(S)^{-m}(b_1a_1)$

Hence $f^{-1}(B) = f^{-1}(R \cup S) = ((f^{-1}(R) \cup f^{-1}(S))^{+m}, (f^{-1}(R) \cup f^{-1}(S))^{-m}))$, is a bipolar valued fuzzy normal sub-bigroup of G_1. ■

Theorem 2.7: *Let $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ be any two bigroups. The anti-isomorphic image of a bipolar valued fuzzy normal sub-bigroup of G_1 is a bipolar valued fuzzy normal sub-bigroup of G_2.*

Proof: Let $f : G_1 \to G_2$ be an anti-isomorphism. Let $A = M \cup N = (M \cup N)^{+m}, (M \cup N)^{-m}$ be a bipolar valued fuzzy normal sub-bigroup of G_1.

By theorem 2.3, $f(A) = ((f(M) \cup f(N))^{+m}, (f(M) \cup f(N))^{-m})$ is a bipolar valued fuzzy sub-bigroup of G_2.

Let $f(a_1)$ and $f(b_1)$ be in G_2. If $f(a_1)$ and $f(b_1)$ are in H_2, then

$$f(M)^{+m}(f(a_1) + f(b_1)) = f(M)^{+m}(f(b_1 + a_1))$$
$$= M^{+m}(b_1 + a_1) = M^{+m}(a_1 + b_1)$$
$$= f(M)^{+m}(f(a_1 + b_1)) = f(M)^{+m}(f(b_1) + (f(a_1))$$

Also, $f(M)^{-m}(f(a_1) + f(b_1)) = f(M)^{-m}(f(b_1 + a_1)) = M^{-m}(b_1 + a_1) = M^{-m}(a_1 + b_1) = f(M)^{-m}(f(a_1 + b_1)) = f(M)^{-m}(f(b_1) + (f(a_1))$

If $f(a_1)$ and $f(b_1)$ are in F_2, then $f(N)^{+m}(f(a_1)f(b_1)) = f(N)^{+m}(f(b_1a_1) = N^{+m}(b_1a_1) = N^{+m}(a_1b_1o9) = f(N)^{+m}(f(a_1b_1) = f(N)^{+m}(f(b_1)f(a_1))$

Also $f(N)^{-m}(f(a_1)f(b_1)) = f(N)^{-m}(f(b_1a_1) = N^{-m}(b_1a_1) = N^{-m}(a_1b_1) = f(N)^{-m}(f(a_1b_1) = f(N)^{-m}(f(b_1)f(a_1))$

Hence $f(A) = ((f(M) \cup f(N))^{+m}, (f(M) \cup f(N))^{-m})$ is a bipolar valued fuzzy normal sub-bigroup of G_2. ■

Theorem 2.8: *Let $(G_1 = H_1 \cup F_1, +, \cdot)$ and $(G_2 = H_2 \cup F_2, +, \cdot)$ be any two bigroups. The anti-homomorphic preimage of a bipolar valued fuzzy normal sub-bigroup of G_2 is a bipolar valued fuzzy normal sub-bigroup of G_1.*

Proof: Let $f : G_1 \to G_2$ be an anti-homomorphism. Let $B = R \cup S = (R \cup S)^{+m}, (R \cup S)^{-m}$ be a bipolar valued fuzzy normal sub-bigroup of G_2. By theorem 2.4, $f^{-1}(B) = f^{-1}(R \cup S) = ((f^{-1}(R) \cup f^{-1}(S))^{+m}, (f^{-1}(R) \cup f^{-1}(S))^{-m})$, is a bipolar valued fuzzy sub-bigroup of G_1. Let a_1 and b_1 be in G_1. If a_1 and b_1 are in H_1, then, $f^{-1}(R)^{+m}(a_1+b_1) = R^{+m}(f(a_1+b_1) = R^{+m}(f(b_1)+f(a_1)) = R^{+m}(f(a_1)+f(b_1)) = R^{+m}(f(b_1+a_1) = f^{-1}(R)^{+m}(b_1+a_1)$.

Also, $f^{-1}(R)^{-m}(a_1+b_1) = R^{-m}(f(a_1+b_1) = R^{-m}(f(b_1)+f(a_1)) = R^{-m}(f(a_1)+f(b_1)) = R^{-m}(f(b_1+a_1) = f^{-1}(R)^{-m}(b_1+a_1)$

If a_1 and b_1 are in F_1, then $f^{-1}(S)^{+m}(a_1b_1) = S^{+m}(f(a_1b_1) = S^{+m}(f(b_1)f(a_1)) = S^{+m}(f(a_1)f(b_1)) = S^{+m}(f(b_1a_1) = f^{-1}(S)^{+m}(b_1a_1)$

Also $f^{-1}(S)^{-m}(a_1b_1) = S^{-m}(f(a_1b_1) = S^{-m}(f(b_1)f(a_1)) = S^{-m}(f(a_1)f(b_1)) = S^{-m}(f(b_1a_1) = f^{-1}(S)^{-m}(b_1a_1)$

Hence $f^{-1}(B) = f^{-1}(R\cup S) = ((f^{-1}(R)\cup f^{-1}(S))^{+m}, (f^{-1}(R)\cup f^{-1}(S))^{-m})$, is a bipolar valued fuzzy normal sub-bigroup of G_1. ■

Theorem 2.9: *Let $A = M\cup N = (M\cup N)^{+m}, (M\cup N)^{-m}$ be a bipolar valued fuzzy sub-bigroup of a bigroup $(G_2 = H_2\cup F_2, +, \cdot)$ and f is an isomorphism from a bigroup $G_1 = H_1\cup F_1$ onto $G_2 = H_2\cup F_2$. Then*

$$A\circ f = A^{+m}\circ f, A^{-m}\circ f = (M^{+m}\circ f)\cup(N^{+m}\circ f), (M^{-m}\circ f)\cup(N^{-m}\circ f)$$

is a bipolar valued fuzzy sub-bigroup of G_1.

Proof: Let a_1 and b_1 be in G_1 and A be a bipolar valued fuzzy sub-bigroup of the bigroup G_2. If a_1 and b_1 in H_1, then,

$(M^{+m}\circ f)(a_1-b_1) = M^{+m}(f(a_1-b_1)) = M^{+m}(f(a_1)-f(b_1)) \geq \min\{M^{+m}(f(a_1)), M^{+m}(f(b_1))\} \geq \min\{(M^{+m}\circ f)(a_1), (M^{+m}\circ f)(b_1)\}$ which implies that $(M^{+m}\circ f)(a_1-b_1) \geq \min\{(M^{+m}\circ f)(a_1), (M^{+m}\circ f)(b_1)\}$

Also $(M^{-m}\circ f)(a_1-b_1) = M^{-m}(f(a_1-b_1)) = M^{-m}(f(a_1)-f(b_1)) \leq \max\{M^{-m}(f(a_1)), M^{-m}(f(b_1))\} \leq \max\{(M^{-m}\circ f)(a_1), (M^{-m}\circ f)(b_1)\}$ which implies that $(M^{-m}\circ f)(a_1-b_1) \leq \max\{(M^{-m}\circ f)(a_1), (M^{-m}\circ f)(b_1)\}$

If a_1 and b_1 are in F_1, then, $(N^{+m}\circ f(a_1{b_1}^{-1}) = N^{+m}(f(a_1{b_1}^{-1})) = N^{+m}(f(a_1)(f(b_1))^{-1}) \geq \min\{N^{+m}(f(a_1)), N^{+m}(f(b_1))\} \geq \min\{(N^{+m}\circ f)(a_1), (N^{+m}\circ f)(b_1)\}$ which implies that $(N^{+m}\circ f)(a_1{b_1}^{-1}) \geq \min\{(N^{+m}\circ f)(a_1), (N^{+m}\circ f)(b_1)\}$

Also $(N^{-m}\circ f)(a_1{b_1}^{-1}) = N^{-m}(f(a_1{b_1}^{-1})) = N^{-m}((f(a_1)f(b_1))^{-1}) \leq \max\{N^{-m}(f(a_1)), N^{-m}(f(b_1))\} \leq \max\{(N^{-m}\circ f)(a_1), (N^{-m}\circ f)(b_1)\}$ which implies that $(N^{-m}\circ f)(a_1{b_1}^{-1}) \leq \max\{(N^{-m}\circ f)(a_1), (N^{-m}\circ f)(b_1)\}$

Hence $A\circ f$ is a bipolar valued fuzzy sub-bigroup of G_1. ■

Theorem 2.10: *Let $A = M\cup N = (M\cup N)^{+m}, (M\cup N)^{-m}$ be a bipolar valued fuzzy subbigroup of a bigroup $G_2 = H_2\cup F_2$ and f is an anti-isomorphism from a bigroup, $G_1 = H_1\cup F_1$ onto G_2. Then $A\circ f = A^{+m}\circ f, A^{-m}\circ f = (M^{+m}\circ f)\cup(N^{+m}\circ f), (M^{-m}\circ f)\cup(N^{-m}\circ f)$ is a bipolar valued fuzzy subbigroup of G_1.*

Proof: Let a_1 and b_1 be in G_1 and A be a bipolar valued fuzzy sub-bigroup of the bigroup $G_2 = H_2\cup F_2$.

If a_1 and b_1 in H_1, then, $(M^{+m}\circ f)(a_1-b_1) = M^{+m}(f(a_1-b_1)) = M^{+m}(f(-b_1)+f(a_1)) \geq \min\{M^{+m}(f(a_1)), M^{+m}(f(b_1))\} \geq \min\{(M^{+m}\circ f)(a_1), (M^{+m}\circ f)(b_1)\}$ which implies that $(M^{+m}\circ f)(a_1-b_1) \geq \min\{(M^{+m}\circ f)(a_1), (M^{+m}\circ f)(b_1)\}$.

Also $(M^{-m}\circ f)(a_1-b_1) = M^{-m}(f(a_1-b_1)) = M^{-m}(f(-b_1)+f(a_1)) \leq \max\{M^{-m}(f(a_1)), M^{-m}(f(b_1))\} \leq \max\{(M^{-m}\circ f)(a_1), (M^{-m}\circ f)(b_1)\}$ which implies that $(M^{-m}\circ f)(a_1-b_1) \leq \max\{(M^{-m}\circ f)(a_1), (M^{-m}\circ f)(b_1)\}$

If a_1 and b_1 are in F_1, then $(N^{+m}\circ f)(a_1{b_1}^{-1}) = N^{+m}(f(a_1{b_1}^{-1})) = N^{+m}((f(b_1))^{-1}f(a_1)) \geq \min\{N^{+m}(f(a_1)), N^{+m}(f(b_1))\} \geq \min\{(N^{+m}\circ f)(a_1), (N^{+m}\circ f)(b_1)\}$ which implies that $(N^{+m}\circ f)(a_1{b_1}^{-1}) \geq \min\{(N^{+m}\circ f)(a_1), (N^{+m}\circ f)(b_1)\}$

Also $(N^{-m}\circ f)(a_1{b_1}^{-1}) = N^{-m}(f(a_1{b_1}^{-1})) = N^{-m}((f(b_1))^{-1}f(a_1)) \leq \max\{N^{-m}(f(a_1)), N^{-m}(f(b_1))\} \leq \max\{(N^{-m}\circ f)(a_1), (N^{-m}\circ f)(b_1)\}$ which implies that $(N^{-m}\circ f)(a_1{b_1}^{-1}) \leq \max\{(N^{-m}\circ f)(a_1), (N^{-m}\circ f)(b_1)\}$

Hence $A\circ f$ is a bipolar valued fuzzy sub-bigroup of G_1. ■

Theorem 2.11: *Let $A = M\cup N = (M\cup N)^{+m}, (M\cup N)^{-m}$ be a bipolar valued fuzzy sub-bigroup of a bigroup $G_2 = H_2\cup F_2$ and f is an isomorphism from a bigroup $G_1 = H_1\cup F_1$ onto G_2. Then we have the following:*

(i) If A is a generalized characteristic bipolar valued fuzzy sub-bigroup of G_2 , then $A\circ f = A^{+m}\circ f, A^{-m}\circ f = (M^{+m}\circ f)\cup(N^{+m}\circ f), (M^{-m}\circ f)\cup(N^{-m}\circ f)$ is a generalized characteristic bipolar valued fuzzy sub-bigroup of G_1.

(ii) If A is a generalized characteristic bipolar valued fuzzy sub-bigroup and f is an automorphism on G_1 , then $A\circ f = A$.

Proof: (i) Let A be a generalized characteristic bipolar valued fuzzy sub-bigroup of G_2. By Theorem 2.9, $A\circ f$ is a bipolar valued fuzzy sub-bigroup of G_1. Let a_1 and b_1 be in G_1. If a_1 and b_1 in H_1 and $o(a_1) = o(b_1)$, then $(M^{+m}\circ f)(a_1) = M^{+m}(f(a_1)) = M^{+m}(f(b_1)) = (M^{+m}\circ f)(b_1)$ which implies that $(M^{+m}\circ f)(a_1) = (M^{+m}\circ f)(b_1)$.

Also $(M^{-m}\circ f)(a_1) = M^{-m}(f(a_1)) = M^{-m}(f(b_1)) = (M^{-m}\circ f)(b_1)$ which implies that $(M^{-m}\circ f)(a_1) = (M^{-m}\circ f)(b_1)$.

If a_1 and b_1 in F_1 and $o(a_1) = o(b_1)$, then $(N^{+m}\circ f)(a_1) = N^{+m}(f(a_1)) = N^{+m}(f(b_1)) = (N^{+m}\circ f)(b_1)$ which implies that $(N^{+m}\circ f)(a_1) = (N^{+m}\circ f)(b_1)$.

Also $(N^{-m}\circ f)(a_1) = N^{-m}(f(a_1)) = N^{-m}(f(b_1)) = (N^{-m}\circ f)(b_1)$ which implies that $(N^{-m}\circ f)(a_1) = (N^{-m}\circ f)(b_1)$.

Hence $A\circ f$ is a generalized characteristic bipolar valued fuzzy sub-bigroup of G_1.

(ii) is clear, as $M^{+m} \circ f = M^{+m}$; $M^{-m} \circ f = M^{-m}$ and $N^{+m} \circ f = N^{+m}$; $N^{-m} \circ f = N^{-m}$ ■

Theorem 2.12: *Let $A = M \cup N = (M \cup N)^{+m}, (M \cup N)^{-m}$ be a bipolar valued fuzzy sub-bigroup of a bigroup $G_2 = H_2 \cup F_2$ and f is an anti-isomorphism from a bigroup, $G_1 = H_1 \cup F_1$ onto G_2. Then we have the following:*

(i) If A is a generalized characteristic bipolar valued fuzzy sub-bigroup of G_2 , then $A \circ f = A^{+m} \circ f, A^{-m} \circ f = (M^{+m} \circ f) \cup (N^{+m} \circ f), (M^{-m} \circ f) \cup (N^{-m} \circ f)$ is a generalized characteristic bipolar valued fuzzy sub-bigroup of G_1.
(ii) If A is a generalized characteristic bipolar valued fuzzy sub-bigroup of G_2 and f is an automorphism on G_1 , then $A \circ f = A$.

Proof: (i) Let A be a generalized characteristic bipolar valued fuzzy sub-bigroup of G_2. By Theorem 2.10, $A \circ f$ is a bipolar valued fuzzy sub-bigroup of G_1.

Let a_1 and b_1 be in G_1. If a_1 and b_1 in H_1 and $(a_1) = (b_1)$, then $(M^{+m} \circ f)(a_1) = M^{+m}(f(a_1)) = M^{+m}(f(b_1)) = (M^{+m} \circ f)(b_1)$ which implies that $(M^{+m} \circ f)(a_1) = (M^{+m} \circ f)(b_1)$.

Also $(M^{-} \circ f)(a_1) = M^{-m}(f(a_1)) = M^{-m}(f(b_1)) = (M^{-m} \circ f)(b_1)$ which implies that $(M^{-m} \circ f)(a_1) = (M^{-m} \circ f)(b_1)$.

If a_1 and b_1 in F_1 and $o(a_1) = o(b_1)$, then $(N^{+m} \circ f)(a_1) = N^{+m}(f(a_1)) = N^{+m}(f(b_1)) = (N^{+m} \circ f)(b_1)$ which implies that $(N^{+m} \circ f)(a_1) = (N^{+m} \circ f)(b_1)$.

Also $(N^{-m} \circ f)(a_1) = N^{-m}(f(a_1)) = N^{-m}(f(b_1)) = (N^{-m} \circ f)(b_1)$ which implies that $(N^{-m} \circ f)(a_1) = (N^{-m} \circ f)(b_1)$.

Hence $A \circ f$ is a generalized characteristic bipolar valued fuzzy sub-bigroup of G_1.

(ii) is clear. ■

3. The proposed encryption method

The extracted shared secret data is extracted once the encryption and decryption processes have been completed in the proposed system. With the help of the encryption technique known as homomorphic encryption, you can add and multiply ciphertexts in order to get this output which match an outcome of similar one. Without disclosing private information for each action, homomorphic encryption enables you to carry out a variety of tasks in an untrusted environment [14]. Encoding messages or information so that only authorized parties can read it is known as encryption in cryptography. Although encryption does not by itself stop interceptions, it does prevent the interceptor from seeing the message's contents. A message or piece of information, known as plaintext in an encryption scheme, is encrypted using an encryption algorithm to create cipher text that can only be decoded and read. An encryption technique typically employs a pseudorandom encryption key produced by an algorithm for technical reasons.

In general, a cryptosystem provides a mechanism to use a secret key to convert one message, known as the plaintext, into another, known as the ciphertext. If the cryptosystem is trustworthy, the plaintext cannot be deciphered by anybody without the secret key, and the ciphertext can be safely made public.

Definition 3.1: A cryptosystem is a five-tuple $(\mathcal{B}, \mathcal{R}, \mathcal{H}, \mathcal{E}, \mathcal{M})$, that meets the requirements listed below:

- $\mathscr{B}$ -finite set of possible plaintexts;
- $\mathscr{R}$ - finite set of ciphertexts;
- $\mathscr{H}$ - finite set of key combinations;
- Encryption rule is defined as $e_{k1} \in \mathcal{E}$ & a corresponding decryption rule $d_{k1} \in \mathcal{M}$ for every $K \in \mathcal{H}$. There are functions for each $e_k : \mathcal{B} \to \mathcal{R}$ and $d_k : \mathcal{R} \to \mathcal{B}$ such that $d_k(e_k(x)) = x$ for each plaintext $x \in \mathcal{B}$.

The Paillier Cryptosystem was found as a result of further investigation into trapdoor discrete logarithm-based cryptosystems that was prompted by the Okamoto-Uchiyama system. The Paillier cryptosystem uses a logarithm function L to decrypt ciphertext and is analogous to the Okamoto-Uchiyama cryptosystem, but it is implemented significantly differently. The Paillier cryptosystem enhances the Benaloh cryptosystem by taking advantage of the difficulty of selecting higher order residues modulo a composite n^2 where $n = pq$.

Lemma 3.1: The class function is a homomorphism from $\mathbb{Z}^*_{n^2}$ *to* $\mathbb{Z}_n$

Proof: Let $w_1, w_2, g \in \mathbb{Z}^*_{n^2}$. Then $[w_1]_g = x_1$ and $[w_2]_g = x_2$ and there exists y_1 and y_2 with $w_1 = g^{x_1}y_1^n$ and $w_2 = g^{x_2}y_2^n$. Set $y = y_1y_2$, then $[w_1w_2]_{g1} = [w_{i1}]_{g1} + [w_{i2}]_{g1} = x_{i1} + x_{i2}$ follows from that fact that $(g^{x_1}y_1^n)(g^{x_2}y_2^n) = g^{x_1+x_2}y^n$.

When the order of g is a multiple of n, the function $\varepsilon_g(x, y) = g^xy^n$ is a bijection from $\mathbb{Z}_n \times \mathbb{Z}^*_n$ to $\mathbb{Z}^*_{n^2}$, and when the order of g is α n *for* $\alpha \in \{1, ..., \lambda = lcm(p-1, q-1)\}$, g decides x for a given g^xy^n. So, using y as a randomizer, ε_g can accept a message x and determine w such that $[w]_g = x$. The class function serves as the Paillier cryptosystem's decryption function, whereas ε_g serves as its encryption function. ■

3.1. Encryption step

When the original data, $D_1, \ldots . D_l$, and secret data D_x are encrypted will produce $l + 1$ encrypted data, $C_1, \ldots, C_l$, and C_x respectively. A new encrypted data is

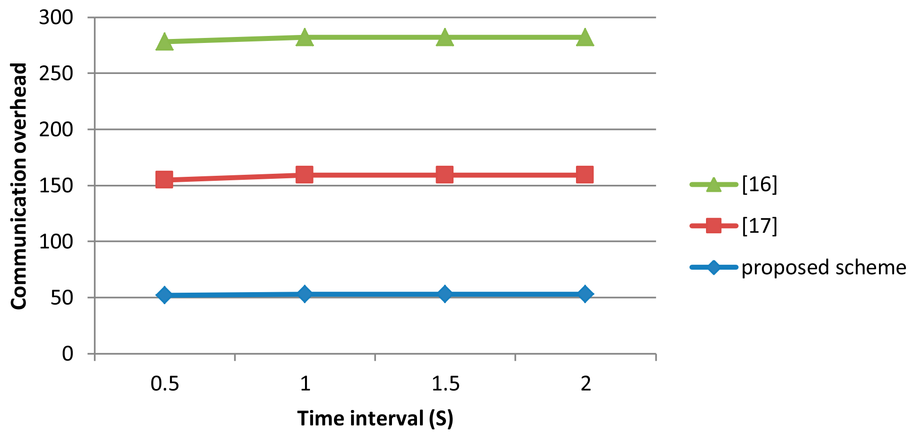

Figure 1. Communication Overhead.

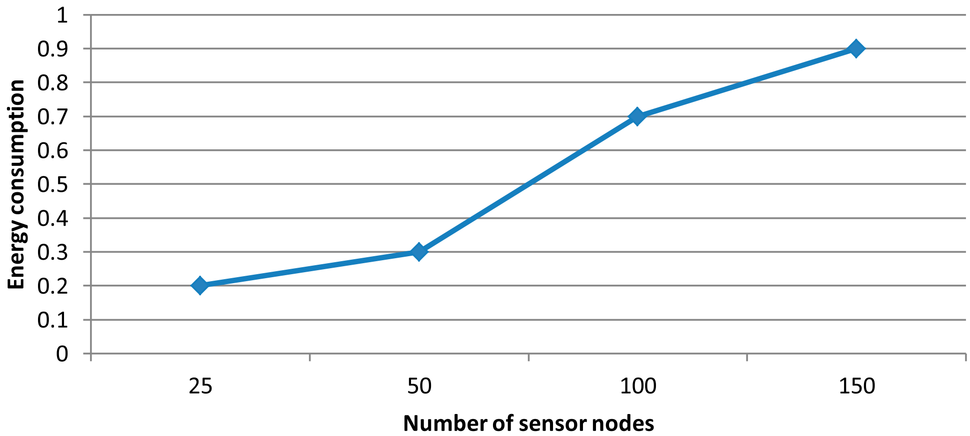

Figure 2. Energy consumption.

created by incrementally multiplying one encrypted data by another encrypted data. Once the secret encrypted data D_x is added, this new encrypted data is put into the homomorphic multiplication procedure to create the final encrypted data C_y. All of the individually encrypted data must be used in order to safeguard the secret data [15–19]. The final encrypted data may have two different sized blocks because two distinct encryption techniques are possible. The Paillier cryptosystem is used with the suggested strategy. It is given by

$$C_y(i) = \left(\prod_{a=1}^{L} C_l(a) \times C_x(a) \right) |n^2| \tag{1}$$

The Paillier cryptosystem uses the n^2 basis for the modulo operation. The blocks $C_y(i)$ are used to create the encrypted image C_y, and the decrypted data D_x is the information we want to transport or exchange across an unsecure channel.

3.2. Decryption part

Our goal is to extract D_x from the $D_1, \ldots\ldots D_l$ and D_y present at the receiving end. According to Paillier's additive homomorphic characteristic,

$$D_y(i) = \left(\sum_{l=1}^{L} D_l(i) + D_x(i) \right) |n| \tag{2}$$

$$D_{x1}(i) = \left(D_{y1}(i) - \sum_{l=1}^{L} D_l(i) \right) |n1| \tag{3}$$

The process is entirely reversible using the Paillier cryptosystem; we can obtain the shared secret data without suffering any loss.

4. Results and discussion

These strategies are put into practice in a simulator designed specifically for WSNs. Because of the message overhead associated with cryptography, the network lifetime is decreased. Each cryptographic primitive has a unique CPU cycle time requirement, which affects how much energy is used during execution.

We contrast the communication costs between our plan and the other two plans. The outcomes are displayed in Figure 1. As a result, we can see that even in the absence of an attack, existing systems incur a very large overhead in transmission and calculation compared to our approach.

Figure 2 shows the energy used by our strategy as well as the energy used by each networked sensor node.

Conclusion

WSNs connect the processing and storage of the data provided by an application process on the appropriate servers. In this work, we looked at how to share a secret data by key-data with exploiting an extra property of homomorphic Pailier crypto system on a bipolarvaluedfuzzy sub-bigroup and the bipolarvaluedfuzzy normal sub-bi-group. The impact of homomorphism and isomorphism over various fuzzy algebraic structures has its own scope for the research work in this area. Still there are so many aspects of homomorphism and isomorphism which can be applied on Bipolar valued fuzzy structures. Here, we will be beneficial for the researchers for their future work in this area. Future work will include investigating and putting various Secured Data Transmission into use, as well as the impact of applying stream cyphers, and making a thorough comparison of the outcomes over WSNs.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

[1] Kuribayashi M, Tanaka H. Fingerprinting protocol for images based on additive homomorphic property. IEEE Trans Image Process. 2005;14(12):2129. doi:10.1109/TIP.2005.859383
[2] Zadeh LA. Fuzzy sets. Inf Control. 1965;8:338–353. doi:10.1016/S0019-9958(65)90241-X
[3] Zhang WR. Bi-polar Fuzzy sets and Relations, A computational frame work for cognitive modeling and multiple decision analysis, Proceedings of Fuzzy IEEE Conferences; 1994, 305(309).
[4] Zhang WR. Bi-polar Fuzzy sets, *Proceedings of Fuzzy IEEE Conferences*; 1998, 835(840).
[5] Lee KM. Bipolarvaluedfuzzy sets and their operations. *Proc. Int. Conf. on Intelligent Technologies, Bangkok, Thailand*; 2000, 307(312).
[6] Lee KM. Comparison of interval-valued-fuzzy sets, intuitionistic fuzzy sets and bi-polarvalued-fuzzy sets. J Fuzzy Logic Intell Syst. 2004;14(2):125–129.
[7] Vasantha kandasamy WB. Smarandache fuzzy algebra. Rehoboth: American research press; 2003.
[8] Anitha MS, Prasad KLM, Arjunan K. Notes on bipolar-valuedfuzzy subgroups of a group. Bull Soc Math Serv Stand. 2013;2(3):52–59.
[9] Balasubramanian A, Prasad KLM, Arjunan K. Notes on intuitionistic fuzzy subbigroup of a bigroup. Int J Sci Res. 2015;4(5):3–5.
[10] Justin Prabu T, Arjunan K. Q-Fuzzy subbigroup of a bigroup. Bull Math Stat Res. 2015;3(2):12–15.
[11] Sheena KP, Devi KU. Bipolarvaluedfuzzy subbigroup of a bigroup. Wutan Huatan Jisuan Jishu. 2021;XVII(III): 134–138.
[12] Alabdulatif A, Kumarage H, Khalil I, et al. Privacy-preserving cloud-based billing with lightweight homomorphic encryption for sensor-enabled smart grid infrastructure. IET Wirel Sensor Syst. 2017;7(6):182–190. doi:10.1049/iet-wss.2017.0061
[13] Balasubramanian A, Prasad KLM, Arjunan K. Homomorphism in Bi-polar interval valued-fuzzy subgroups of a group. Int J Math Arch. 2015;6(4):201–204.
[14] Sen J. (2013). Homomorphic encryption: theory and application theory and practice of cryptography and network security protocols and technologies; pp 31; 2012.
[15] Anitha MS, Prasad KLM, Arjunan K. Homomorphism and anti-homomorphism of bipolarvaluedfuzzy subgroups of a group. Int J Math Arch. 2013;4(12):1–4.
[16] Rappe D. Homomorphic cryptosystems and their applications, *Cryptology ePrint Archive, Report 2006/001*; *2006*.
[17] Parmar K, Jinwala DC. Aggregate MAC based authentication for secure data aggregation in wireless sensor networks. Lect Notes Comput Sci. 2014;8589(4):475–483. doi:10.1007/978-3-319-09339-0_48
[18] Engouang TD, Yun L. (2013). Aggregate over multi-hop homomorphic encrypted data in wireless sensor networks. Proceedings of the 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation, Toronto, Canada, 248–252.
[19] Islam N, Puech W, Hayat K, et al. Application of homomorphism to secure image sharing. Opt Commun. 2011;284(19):4412–4429. doi:10.1016/j.optcom.2011.05.079