Conglomerate Energy Efficient Elgamal Encryption Based Data Aggregation Cryptosystems in Wireless Sensor Network

T. G. Babu*†, V. Jayalakshmi

* Department of Computer Applications, Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai, India

1. INTRODUCTION

WSN comprise huge number of sensor nodes and are widely distributed in the sensor environment for evaluating and receiving data. The sensor nodes are controlled by Base Station (BS) and are used to monitor the environment and transmit the sensed data requested by the recipient node through BS [1]. WSN has been utilized in various application such as defence domain, medical field, weather forecasting and several other industrial and commercial applications [2]. The WSN sensors are generally compact and utilize limited battery constraint. The sensor aggregates the data and transmits to the server location which is stated as the base station. At the base station the data received are analysed to create a decision for several prescribed application. These nodes function as a repeated for transmitting the data to other sensors and sink. Further WSN power source must be utilized in an appropriate way since it could not be recharged or exchanged. These WSN frameworks are affected by several parameters such as fault tolerance, energy efficiency, scalability etc. The WSN sensors exhaust the energy mainly in two kinds of ways which are environmental parameter sensing and data transmission to base station through the sensor nodes. The inadequate power source are regarded as the key issue in wireless sensor network and hence the network failure and node failure arises [3]. Further the optimal energy usage in WSN is needed for obtaining high lifetime and more performance. So grouping of sensors into the corresponding clusters has been employed for decreasing the network energy consumption and thereby to increase the network reliability. Every Cluster possesses Cluster Head and an

*Corresponding Author Email: babuit.17@gmail.com (T. G. Babu)
effective framework like our proposed system is required to reduce the consumption of energy. ElGamal encryption is the public key cryptographic algorithm used for secure exchanging of information between two parties which is based on D-H key exchange. However, ElGamal algorithm uses one way hash function and it is very difficult to break the encryption and the attacker cannot inverse the hash function to get the original message. Merkle–Hellman algorithm is one of the earliest public key algorithm based on sub-set sum problem which is now considered insecure after the evolution of many public key algorithm like RSA. The proposed system utilized ElGamal based encryption that enable effective data aggregation [4, 5]. ElGamal cryptosystem modifies Diffe Hellman protocol and employs Digital Signature Algorithm for signing digital documents. It comprises major process like effective key generation, encryption and decryption system. Its non-deterministic encryption the same plaintext multiple times will result in different cipher texts, since a random k is chosen each time [6, 7]. The cryptosystem needs one is Public key which is used for Encryption process and the other one is Private key which is used for Decryption process [8]. The algorithm in turn uses “Energy” as a parameter to find out the better routing to reach the destination. Normal nodes only communicated with its neighbour and every node will take data fusion in order. The distance of the connect nodes with each other have been shortened remarkably. Nodes take turns to be the cluster head, so it takes no energy. In this research work, the combination of ElGamal based encryption followed by data aggregation and Knapsack based Energy efficient AODV promotes the overall effectiveness of the cryptosystem. The main contribution of the proposed work are

- To frame an effective Conglomerate ElGamal based encryption associated with multiple key generations that allows reliable data aggregation and more security.
- To increase the performance of the network through secure transmission of keys with energy efficient strategy.

The organisation of the paper is as follows. Initial section provides the introduction and need for the study. Section 2 provides the survey of existing literature in accordance with the proposed work. Section 3 describes the methodology and section 4 offers the performance analysis of the proposed system. Section 5 concludes the work in detail:

2. REVIEW OF LITERATURE

This section provides the survey of prevailing works in accordance to the proposed system. Ara et al. [9] suggested a secured privacy preservation data aggregation system in accordance with bilinear pairing for improving data privacy and data aggregation efficiency. The suggested system has been proved to be secured under Diffe Hellman assumption. Further it utilized Elgamal cryptosystem for secured encryption. The suggested system showed effective data aggregation with reliable computational cost. Wang et al. [10] suggested a clustering algorithm for the selection of cluster heads with an enhanced ABC algorithm. The study introduced cluster head density, energy, location and other such similar factors into the suggested framework. This enhanced ABC has been utilized for the optimization of fuzzy c means to determine the effective clustering method. The study also employed an Ant colony based energy efficient routing protocol to improve network throughput. The study introduced a polling controlling mechanism to intra-cluster communication process. Agarkar et al. [11] presented a security mechanism based on lattice cryptography for data aggregation for WSN. It employed learning with errors over the rings for encryption of data. The security analysis employed that the suggested system offered integrity, confidentiality and authenticity during the process of communication. The efficiency of this lightweight system depicted that it is more better than ElGamal cryptosystem. Hamza and Al-Alak [12] used Kaiser Constant Modulus Algorithm (KCMA) technique for the generation of twelve experiments of Elgamal, Rivest Shamir Adleman (RSA) and Electrical Computer and Communication (ECC) algorithms. These chain of experiments merged with the hash function XOR and Secure Hash Algorithm 2 (SHA2). The study utilized Diehard test in the experiments for the evaluation of randomness of the generated secret key thereby displaying the security of the system. The study determined that SHA2 has been found to be better than XOR. Further the work assesses the efficiency time for the throughput network. Wang et al. [13] deliberated an reliable and efficient WSN clustering algorithm on the basis of quantum artificial bee colony (ABC) algorithm that aimed at unbalanced load in WSN clustering without the consideration of residual node energy, node position and node intensity. This algorithm could be able to adapt better to the network topology and also decreased the node energy consumption and extend the network lifetime. The experimental outcomes of the represented that the algorithm increased the stability of the overall system. The work aimed to further improve the algorithm for the data acquisition and network clustering of mobile WSN. Leelavathi et al. [14] investigated encryption of image and text data that has been embedding as elliptic curve point. The finite field arithmetic has been used effectively in the suggested cryptosystem. The pre computations for the image input conversion and text data has been performed with the use of MATLAB. Here the message size differs with various stream size and also
the mapping of input data has been presented with high security that indicates less vulnerability in attacks. The study also performed statistical analysis on the encrypted and plain images for assessing the strength of the suggested method.

Asma and Lehsaini [15] suggested an energy effective routing algorithm for balancing the energy during forwarding the information from source to the corresponding link. The system offered better effectiveness when compared to the prevailing routing algorithms in accordance to energy efficacy. The study also extended the network lifetime of WSN. The simulation results of the study depicted that knapsack based energy efficient system will be greatly utilised for addressing data aggregation problems. In future the study attempted to deal with the security issues for misbehaving nodes. Xing et al. [16] investigated a private data aggregation system on the basis of homomorphic encryption and digital signatures. This paper possess the capability of verifying the information from various nodes that have identifiability. Further confidentiality interference factor technique was introduced for defending the interior attack. Next the study adopted a homomorphic encryption property based on confidentiality sum algorithm without trust party. This avoided efficiency and safety problem that results from trusted third party. Finally the study provided the security proof and effectiveness analysis for the suggested scheme.

Prabu [17] investigated knapsack algorithm for avoiding brute drive attack through growing confusions. The modules are combined for performing knapsack encryption and decryption, matrix mapping and de-mapping. The study utilized Verilog language for simulation and coding on Spartan 6 and Xilinx ISE. Entire cryptosystem has been executed with the frequency of 503 MHz. When compared with the previous work, the utilization area is found to be very less thereby satisfying the resource parameters of WSN. Al-Naame and Ali [18] suggested a Cluster based data aggregation methodology in WSN that utilized Elliptical Curve Cryptography based on ElGamal homomorphic cryptosystem for the provision of integrity and confidentiality. This deliberated work offered security against several possible malicious behaviour and possible attacks with extended network lifetime. Maheshwari et al. [19] investigated the data aggregation efficiency for developing cluster-based routing algorithm for achieving the low energy consumption for data aggregation and security problems in WSN. The study analysed routing, clustering and protection protocol that is effective against the existing method. WSNs are also vulnerable to several threats and attacks. Among these, congestion is a serious form of attack that disrupts and collapses a WSN very deeply. This, in turn, causes tremendous increase in the rate of packet drops and also results in very high. In order to overcome the limitations of the existing works the presented proposed work attempted a better approach.

3. THE PROPOSED METHODOLOGY

The proposed methodology has been explained in this section with an explorative flow diagram in Figure 1.

The transmitting data are processed with prime number primitive root creation. The proposed key generation algorithm utilize one large prime number ‘q’, which is greater than size of the message ‘n’. The set of primitive roots of prime number ‘q’ is determined. This is followed by the generation of public key and private key. This study employed ElGamal based conglomerate encryption and decryption. The encryption phase has been processed for cluster head selection. The developed cluster member was used for the determination of cluster weight and data acquisition. By performing aggregation logic the members were subjected to data aggregation phase. The transferred aggregated data has been subjected to performance analysis for the evaluation of the proposed method.

3. 1. Data Aggregation Based Conglomerate ElGamal Encryption

ElGamal encryption is a public key cryptographic system and utilize asymmetric key encryption for the communication purpose in between the two parties and for encrypting the message [20, 21]. This was introduced by TaherElGamal in 1985 and is a probabilistic algorithm developed on the basis of Diffie-Hellman key exchange method. This exists a comprehensive encryption-decryption system which depend on discrete logarithm issues. A probabilistic encryption could be defined as the encryption system which develops the various ciphertexts when the similar plaintext is encrypted various times and the discrete logarithm issue is determining the discrete logarithm to the group base. The data aggregation based ElGamal encryption system is defined below. Here the algorithmic steps for encryption, data aggregation and

![Figure 1. Overview of the ElGamal Scheme](image-url)
decryption of the aggregated data has been deliberated below.

**Algorithm I:** Data aggregation based Elgamal Encryption

**Input:** sensors data $S^p_{BS}$

**Output:** Aggregated Data $D_{aggr}$, encrypted data $S^c_i$ and decrypted data $S^r_i$

**Procedure:**

1. **Key generation:**
   - Choose large prime number $p$
   - Choose a primitive value $g$ in modulo $p$
   - Randomly choose $m$, such that $2 \leq m \leq p - 2$
   - Now computes the secret integer, $c = mod(g^m, p)$
   - The combined public keys are $(g, c, p)$
   - The private keys are $(m, p)$

2. The sensed data is encrypted with public keys, the following process are performed during encryption process,$$
S^c_i = c \mod p \\
S^r_i \equiv S^c_i \mod p
$$
3. Perform data aggregation process for all sensed data,
   $$
   D_{aggr} = S^c_1 + S^c_2 + \cdots + S^c_i
   $$
4. Apply decryption process for aggregated data,
   $$
   S^r_i = D_{aggr} \cdot c^m \mod p
   $$
5. The usage of energy for transmitting their sensed
   $$
   E_{TX}(m, d_i) = \begin{cases}
   E_{elec} + m \delta_f d_i^2 d_i \leq \rho \\
   E_{elec} + m \delta_f d_i^2 d_i > \rho
   \end{cases}
   $$

Where,
- $\delta_f$ – the free space
- $\delta_m$ – multipath fading channel model
- $E_{elec}$ – electronic energy which is based on some factors includes the modulation and digital coding
- $\rho$ – threshold distance

6. Find the generation of CH selection based on the multi objective fitness function of knapsack
   problem with two parameters such as residual
   energy and sensing range $\varphi$
   $$
   fit\_val = c_1 \left( \frac{E_{m}^{r} - E_{i}^{r}}{E_{m}^{r}} \right) + c_2 \left( \frac{\varphi_{m}^{i} - \varphi_{i}^{i}}{\varphi_{m}^{i}} \right)
   $$

Where, $E_{m}^{r}$ – maximum residual energy
- $E_{i}^{r}$ – residual energy for sensors
- $\varphi_{m}^{i}$ – maximum sensing range and $\varphi_{i}^{i}$ sensing range of each sensor

The sensor nodes are deployed and all the nodes and base stations are in stationary mode. The presented paper utilized a simplified model for the consumption of communication energy. On depending on the distance in between the receiver and transmitter, the free space or the multipath fading channel method were employed. The energy required for transmitting the packet over distance has been estimated in the algorithm in step 7. The electronic energy relies on few factors comprising the modulation and digital coding whereas the amplifier energy relies on the transmitting distance. In order to receive such kind of packets the radio consuming energy has been determined in step 8. After random deployment, random number of nodes were chosen on the basis of probability for the selected node $S^c_i$. Based on the equation provided in step 8 the random nodes are chosen. Followed by that neighboring nodes on the basis of minimum Euclidean distance was selected with the step 10 which provides the distance between random nodes and member nodes.

4. PERFORMANCE ANALYSIS

The experimental setup and performance of the proposed method are discussed in this section. The performance of the cluster based routing is analyzed using various metrics alive nodes, dead nodes, average energy consumption, total packet sent, and throughput. Existing LEACH protocol has been utilized for comparison. Table 1 shows the simulation parameters. The performance measures are explained as follows:

- **Alive nodes based on energy:** Alive nodes define the number of nodes that are alive in the network. The network performance is improved, when the network has a high number of alive nodes.

- **Average energy consumption:** It defines the average amount of energy consumed by each node during each iteration.

- **Total packets transmitted to the BS:** The total packets transmitted to BS are directly proportional to the alive nodes and residual energy of the nodes. The total packets received by BS are high when alive nodes are high.

- **Throughput:** The throughput is defined as the amount of bits transmitted to BS over WSN. Throughput is measured as bits per second. Packet drop ratio: The packet drop ratio is defined as the volume of packet loss occurred during the transmission from source node to the BS.

Figure 2 shows the coverage area and Figure 3 shows the initial node deployment. In Figure 4, the total energy consumption in Joules for the proposed system has been evaluated for different rounds. It has been observed that the energy consumption increases with an increase in rounds and time. The energy consumption for 300 milliseconds has been found to be 0.025 J which is less than the existing systems. Hence the proposed system proves to be efficient in terms of energy consumption. The overall network of the proposed system at various nodes was evaluated in Figure 5. The network lifetime seems to be decreases for the processing rounds from 50 milliseconds to 300 milliseconds. It was observed that the network lifetime varies between 11000 milliseconds to 2500 milliseconds.
TABLE 1. Simulation Parameters

| Simulation Parameters       | Values              |
|----------------------------|---------------------|
| Simulation Area            | 200 * 200           |
| Density of Nodes           | 1000 to 1500        |
| Transmission range         | 20-30 ms            |
| Radio Propagation Model    | Two Ray Model       |
| Environment                | Urban               |
| Node Initial Energy        | 150 J               |
| Transmission Power (tx)    | 1.5 J per packet    |
| Receiving Power (rx)       | 0.48 J per packet   |
| Simulation Duration        | 50 Minutes          |
| No of trails               | 65                  |
| Packet Size                | 30 Bytes            |

The average energy analysis for the proposed system has been assessed for the proposed system in Figure 6. It was observed that the average energy of each node of the proposed system has been observed to be more that the existing system. Due to the prevalence of more energy, the proposed system performs better in terms of performance parameters. Dead node is a generated node that is not to be expanded or explored any further. All children of a dead node have already been expanded. Figure 7 deliberates the dead node analysis for the proposed and existing system. It was observed that the existing approach has earlier dead nodes when compared to the proposed system.

Table 2 deliberates the security analysis through assessing several characteristics depicted in that table. Resiliency, efficiency, digital ledger, decentralization, smart contract and anonymity characteristics were assessed in accordance to problems such as third party access, eavesdropping, availability, single point failure, trust, immutability, botnet attacks and data privacy. These assessment proves the effective functioning of the proposed system.

Figure 8 offers a comparative assessment of the proposed method with the state of art method in terms of residual energy. This assessment proved the effectiveness of the proposed system.
Figure 6. Average Energy Analysis

Figure 7. Alive node analysis

| Characteristics          | Resiliency | Efficiency | Digital Ledger | Decentralization | Transparent & Verifiable | Smart Contract | Anonymity |
|--------------------------|------------|------------|----------------|------------------|--------------------------|----------------|-----------|
| Third Party              | Yes        | No         | Yes            | No               | Yes                      | No             | Yes       |
| Eavesdropping            | No         | No         | No             | Yes              | No                       | No             | Yes       |
| Access Control           | Yes        | Yes        | NO             | No               | Yes                      | No             | Yes       |
| Availability             | Yes        | Yes        | Yes            | Yes              | Yes                      | Yes            | Yes       |
| Integrity of Data        | No         | Yes        | Yes            | No               | No                       | No             | Yes       |
| Single Point failure     | No         | Yes        | Yes            | Yes              | No                       | Yes            | No        |
| Trust                    | Yes        | Yes        | No             | No               | Yes                      | Yes            | No        |
| Botnet Attacks           | No         | No         | No             | Yes              | No                       | Yes            | Yes       |
| Immutability             | No         | Yes        | Yes            | Yes              | No                       | No             | No        |
| Data Privacy             | Yes        | Yes        | No             | No               | Yes                      | Yes            | Yes       |

5. CONCLUSION

Data aggregation plays a vital role in WSN and also possess greater impact on the data transferring between the sensor nodes. ElGamal cryptosystem modifies Diffie Hellman protocol and employs Digital Signature Algorithm for signing digital documents. Hence the paper focussed on the integration of Conglomerate ElGamal Encryption and indicating the way of energy efficient protocol has been used and the performance of the proposed system are evaluated. The performance parameters such as packet delivery ratio, throughput, estimation of alive nodes and dead nodes for different rounds has been performed in the study. The efficacy of proposed framework has been compared with state of art methods in terms of residual energy and depicted that
deliberates the superior performance of the presented framework.

6. REFERENCES

1. Khan, T., Singh, K.J.I.o.D.M.S. and Cryptography, "Resonant management based secure trust model for wsns", Journal of Discrete Mathematical Sciences and Cryptography Vol. 22, No. 8, (2019), 1455-1462, doi: 10.1080/09720529.2019.1695897

2. Alkalbani, A.S. and Mantors, T., "Security comparison between dynamic & static wsns for 5g networks", in 2017 Second International Conference on Informatics and Computing (ICIC), IEEE. (2017), 1-4.

3. Mosavvar, I. and Ghaffari, A.J.W.P.C., "Data aggregation in wireless sensor networks using firefly algorithm", Wireless Personal Communications Vol. 104, No. 1, (2019), 307-324, doi: 10.1007/s11277-018-6021-x

4. Hayouni, H., Hamdi, M.J.I.A., and Computing, S., "A data aggregation security enhancing scheme in wsns using homomorphic encryption", Intelligent Automation & Soft Computing, (2017), 1-9, doi: 10.1080/10798587.2017.1327157

5. Randhawa, S. and Jain, S.J.W.P.C., "Data aggregation in wireless sensor networks: Previous research, current status and future directions", Wireless Personal Communications Vol. 97, No. 3, (2017), 3355-3425, doi: 10.1007/s11277-017-4674-5

6. Sariya Praba, T., Meena, V., Sethukarasi, T., Prachetha, K., Aravind, B., Bharathkumar, K.J.I.o.L and Systems, F., "Energy measure cluster based concealed aggregation for confidentiality and integrity in wsns", Journal of Intelligent & Fuzzy Systems Vol. 38, No. 5, (2020), 6475-6482, doi: 10.3233/JIFS-179728

7. Vidhya, S., Sasiathna, T.J.I.J.o.C., and Nanoscience, T., "Performance analysis of ad-hoc on demand distance vector and energy power consumption in wireless sensor networks", Journal of Computational and Theoretical Nanoscience Vol. 14, No. 3, (2017), 1265-1270, doi: 10.1166/jctn.2017.6442

8. Sowmyadevi, D. and Karthikeyan, K., "Merkle-hellman knapsack-side channel monitoring based secure scheme for detecting provenance forgery and selfish nodes in wireless sensor networks", in 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), IEEE. (2017), 1-8.

9. Ara, A., Al-Rodhaan, M., Tian, Y. and Al-Dhaalan, A.J.I.A., "A secure privacy-preserving data aggregation scheme based on bilinear elgamal cryptosystem for remote health monitoring systems", Vol. 5, (2017), 12601-12617, doi: 10.1109/ACCESS.2017.2716349

10. Wang, Z., Ding, H., Li, B., Bao, L. and Yang, Z.J.I.A., "Any energy efficient routing protocol based on improved artificial bee colony algorithm for wireless sensor networks", Vol. 8, (2020), 133577-133596, doi: 10.1109/ACCESS.2020.3010313

11. Agarkar, A.A., Karyakarte, M. and Agrawal, H., "Post quantum security solution for data aggregation in wireless sensor networks", in 2020 IEEE Wireless Communications and Networking Conference (WCNC), IEEE. (2020), 1-8.

12. Hamza, A.H. and Al-Alak, S.M.K., "Evaluation key generator of multiple asymmetric methods in wireless sensor network (wsns)", in Journal of Physics: Conference Series, IOP Publishing. Vol. 1804, No. 1, (2021), 012096.

13. Wang, H., Chen, Y. and Dong, S.J.I.W.S.S., "Research on efficient efficient routing protocol for wsns based on improved artificial bee colony algorithm", Vol. 7, No. 1, (2017), 15-20, doi: 10.1049/iet-wss.2016.0006

14. Leelavathi, G., Shaila, K., Venugopal, K.J.I.J.o.V.I. and Systems, C., "Reconfigurable hardware architecture of public key crypto processor for vanet and wireless sensor nodes", International Journal of Vehicle Information and Communication Systems Vol. 5, No. 1, (2020), 11-25, doi: 10.1004/ijvics.2020.107179

15. Chikh, A., Lehsaini, M.J.C., Practice, C. and Experience, "Combination of greedy and compass approaches for efficient multipath geographic routing in wireless multimedia sensor networks", Online First, (2021), e6703, doi: 10.1002/cpe.6703

16. Li, X., Chen, D., Li, C. and Wang, L.J.S., "Secure data aggregation with fully homomorphic encryption in large-scale wireless sensor networks", Vol. 15, No. 7, (2015), 15992-15973, doi: 10.3390%2Fs150715952

17. Prabu, J., "An energy efficient secure data aggregation in wireless sensor networks", (2021), doi: 10.21037/iee.2021.26-364741/v1

18. Al-naamee, M.K., Ali, S.M.J.B.o.E.E. and Informatics, "Improved el gamal public key crytostystem using 3d chaotic maps", Bulletin of Electrical Engineering and Informatics Vol. 10, No. 1, (2021), 404-411, doi: 10.11591/eei.v10i1.2124

19. Maheshwari, P., Sharma, A.K. and Verma, K.J.A.H.N., "Energy efficient cluster based routing protocol for wsns using butterfly optimization algorithm and ant colony optimization", Ad Hoc Networks Vol. 110, (2021), 102317, doi: 10.1016/j.adhoc.2020.102317

20. Talebi, Z. and Timarchi, S.J.I.J.o.E., "Improved distributed particle filter architecture with novel resampling algorithm for signal tracking", International Journal of Engineering, Transactions C: Aspects, Vol. 33, No. 12, (2020), 2482-2488, doi: 10.5829/jie.2020.33.12c.07

21. Bypour, H., Farhadi, M. and Mortazavi, R.J.I.J.o.E., "An efficient secret sharing-based storage system for cloud-based internet of things", International Journal of Engineering, Transactions B: Applications Vol. 32, No. 8, (2019), 1117-1125, doi: 10.5829/jie.2019.32.08b.07
پیش‌بینی سیم‌های حساس و رایگان است که همچنین بر انتقال داده بین گره‌های حساس تأثیر می‌گذارد. مسئله‌ای که در این مقاله بررسی می‌شود، شکستگی سیم و حمله‌های قبلاً معرفی شده است. در این مقاله، به بهبود عملکرد گره‌های WSN و به نرم‌افزارهای امنیتی متمایز رویکرد می‌گیریم.

توضیحات: 

WSN، این نرم‌افزارهای امنیتی به منظور انتقال داده به کارنامه‌های موجود برای رسیدگی به مسائل امنیتی در WSN کامل می‌باشد. این نرم‌افزار به‌طور جایگزینی یا به‌طور مشتق‌سازی می‌تواند به عنوان یک راه حل کارآمد برای افزایش عملکرد سیستم‌های حساس به‌طور فعال یا مشتق‌سازی استفاده شود. 

SAM (Simm) 

SAM یک نرم‌افزاری است که به‌طور مشتق‌سازی می‌تواند به عنوان یک راه حل کارآمد برای افزایش عملکرد سیستم‌های حساس به‌طور فعال یا مشتق‌سازی استفاده شود. 

SAM یک نرم‌افزاری است که به‌طور مشتق‌سازی می‌تواند به عنوان یک راه حل کارآمد برای افزایش عملکرد سیستم‌های حساس به‌طور فعال یا مشتق‌سازی استفاده شود. 

SAM یک نرم‌افزاری است که به‌طور مشتق‌سازی می‌تواند به عنوان یک راه حل کارآمد برای افزایش عملکرد سیستم‌های حساس به‌طور فعال یا مشتق‌سازی استفاده شود.