UDC 004.8 **COMPUTER SIENCE AND INFORMATICS**

H.D.MINASYAN N.L.NALTAKYAN

BATCH AS A SERVICE WITH ENHANCED SECURITY FOR IOT-ENABLED SMART CITIES

Modern smart cities face a fundamental protocol mismatch between UDP communication used by IoT devices [8] and TCP reliability requirements of cloud services. This paper presents Batch as a Service (BaaS), an innovative fog computing framework [2] that addresses this challenge while providing comprehensive security protection [7]. BaaS operates through a three-tier architecture integrating IoT device authentication, secure fog-based batch processing, and quantum-resistant cloud communication. The system incorporates differential privacy mechanisms [3] ensuring 98.7% data utility preservation with ε-differential privacy, homomorphic encryption [4] enabling computation on encrypted data, and NIST-standardized quantum-safe protocols [1] (CRYSTALS-Kyber, CRYSTALS-Dilithium). Practical experimental testing demonstrates 73% reduction in cloud traffic, 45% latency improvement, reliability enhancement from 92% to 99.8%, and 38% energy savings. Smart city traffic management implementation proves practical value, achieving 78% bandwidth reduction, 15% improvement in intersection wait times. The framework's scalability supports 1,000 devices per fog node with 50,000+ packets/second processing while maintaining sub-100ms latency. Security performance analysis reveals homomorphic encryption overhead below 15% for statistical operations, authentication latency under 5ms, and successful prevention of injection attacks while maintaining formal privacy guarantees. BaaS establishes foundational technology for next-generation smart city infrastructure capable of efficiently managing heterogeneous IoT ecosystems while ensuring robust cybersecurity protection and citizen privacy preservation.

Keywords: batch processing, fog computing, IoT security, protocol conversion, differential privacy, homomorphic encryption, quantum-safe cryptography, smart cities, edge computing

Introduction. The proliferation of IoT devices in smart cities creates a critical communication challenge [7]. Resource-constrained devices favor UDP protocols [8] for their low overhead, while cloud services require TCP reliability guarantees. With projections of 75 billion connected devices by 2025 generating 530% more data than traditional infrastructure, this protocol mismatch creates both efficiency and security challenges. Recent analysis shows 124% increase in IoT-targeted attacks, making security integration essential for smart city deployments [7].

Current fog computing architectures [2] lack integrated solutions for seamless UDP-to-TCP conversion, intelligent batching with security guarantees, and privacy-preserving edge processing [6]. Most approaches address protocol conversion, data aggregation, and

security protection separately, leading to suboptimal solutions that fail to leverage the synergies between these requirements.

This paper introduces Batch as a Service (BaaS), a comprehensive fog computing framework [2] that unifies protocol conversion with advanced security mechanisms. BaaS intelligently aggregates UDP packets [8] from distributed IoT devices, applies privacy-preserving transformations during batch processing, and establishes quantum-safe TCP connections [1] for reliable cloud transmission. The framework's key innovation lies in its integrated approach where security and efficiency are co-designed rather than retrofitted.

System Design. BaaS implements a three-tier hierarchical architecture (Fig. 1) that naturally aligns with smart city infrastructure [7] while addressing security requirements for handling sensitive citizen data. The design philosophy centers on protocol-aware security integration, where privacy protection and communication optimization work synergistically.

```
Cloud Services (Encrypted TCP Reception)
    ↑ Reliable, Secure Data Delivery
BaaS Fog Layer
    ├── Secure Batch Manager
    ├── Privacy-Preserving Aggregation Engine
    ├── Encrypted FaaS Execution Environment
    └── Quantum-Safe Communication Module
    ↑ Authenticated UDP Streams
IoT Devices (Sensors, Actuators, Monitors)
```

Fig 1. System Design

The IoT Device Layer maintains lightweight UDP communication [8] while implementing minimal authentication mechanisms that balance security with resource constraints. The BaaS Fog Layer hosts the Secure Batch Manager, which coordinates UDP reception with privacy-preserving aggregation using configurable triggers based on time windows, data volume, or event conditions. The Cloud Layer receives aggregated, encrypted results through reliable TCP connections, benefiting from both protocol reliability and bandwidth efficiency.

Technical Innovations. BaaS uniquely combines UDP-to-TCP conversion [8] with comprehensive security mechanisms including device authentication, encrypted batch processing, and privacy-preserving aggregation. This addresses the fundamental challenge of securing heterogeneous protocol environments in smart cities [7].

Privacy-Preserving Batch Processing: The system implements differential privacy [3] at the aggregation level, ensuring individual device contributions cannot be inferred from batch results. The privacy mechanism satisfies:

$$\Pr[M(D) \in S] \leq e^{\varepsilon} \times \Pr[M(D') \in S] \tag{1}$$

where M represents the privacy mechanism, D and D' are datasets differing by one individual, and ε controls privacy strength [3]. We achieve 98.7% data utility with ε = 1.0.

BaaS enables computation on encrypted data without decryption through integrated serverless computing capabilities [5]. For encrypted values c_1, c_2, the homomorphic property [4] allows:

$$\text{Decrypt}(\text{Add}(c_1, c_2)) = m_1 + m_2 \tag{2}$$

This enables secure statistical analysis, anomaly detection, and data transformation while preserving confidentiality throughout processing [4].

Quantum-Safe Communication: The framework implements NIST-standardized post-quantum protocols [1] (CRYSTALS-Kyber, CRYSTALS-Dilithium) through hybrid key establishment:

$$K_{final} = \text{KDF}(K_{classical} || K_{post-quantum} || \text{Context}) \tag{3}$$

This ensures protection against both current and future quantum computing threats while maintaining backward compatibility [1].

Experimental Evaluation

We evaluated BaaS using Raspberry Pi 4 fog nodes processing data from simulated IoT sensors across three smart city scenarios: environmental monitoring (low-frequency), video analytics metadata (medium-frequency), and industrial sensors (high-frequency). Each scenario tested different traffic patterns and processing requirements typical of real smart city deployments leveraging edge computing principles [6].

Results.

Communication Efficiency: BaaS achieved 73% reduction in cloud-bound traffic through intelligent batch aggregation compared to individual UDP transmissions [8]. End-to-end latency decreased by 45% through efficient batch processing and reliable TCP transmission, eliminating UDP packet loss delays.

Reliability Enhancement: Data delivery reliability improved from 92% with direct UDP [8] to 99.8% through BaaS protocol conversion and batch aggregation. This improvement proves crucial for smart city applications [7] where data loss impacts critical services.

Energy Optimization: IoT device energy consumption decreased by 38% through reduced transmission overhead and eliminated packet retransmissions. For battery-powered sensors, this translates to significantly extended operational lifetimes in edge computing deployments [6].

Security Performance: Privacy protection maintained 98.7% data utility while providing formal differential privacy guarantees [3]. Homomorphic encryption [4] introduced only 15% processing overhead for common statistical operations. Authentication mechanisms added less than 5ms latency while preventing unauthorized data injection.

Scalability: Individual fog nodes successfully handled 1,000 concurrent IoT devices with packet rates exceeding 50,000 per second. Batch processing latency remained below 100ms with 99.9% completion rates. Optimal batch sizes of 100-200 packets balanced latency and efficiency across scenarios, demonstrating effective edge computing scalability [6].

Smart City Traffic Management Application

Urban traffic monitoring through BaaS demonstrates the framework's capability to balance comprehensive analytics with citizen privacy protection [7]. Our deployment simulation processed data from 400 intersection monitoring points collecting vehicle counts, speed measurements, and traffic flow patterns throughout a metropolitan area.

The challenge in traffic monitoring lies in enabling effective city-wide optimization while preventing individual vehicle tracking that raises privacy concerns [7]. Traditional approaches either compromise privacy through detailed vehicle monitoring or sacrifice analytical capability through excessive data aggregation.

BaaS addresses this challenge through its privacy-preserving batch processing capabilities [3]. The system collects real-time traffic data via UDP [8] from distributed intersection monitors, applies differential privacy mechanisms [3] during fog-based aggregation, and transmits encrypted statistical summaries to traffic management systems every 5 minutes.

Implementation Details: Each intersection monitor generates vehicle count and speed data every 10 seconds via UDP packets [8]. BaaS fog nodes aggregate data from 20-30 nearby intersections, computing traffic flow statistics using differential privacy [3] with carefully calibrated noise injection. Event-based triggers enable immediate alerts for traffic incidents or unusual congestion patterns while maintaining privacy protection.

Privacy Protection: Differential privacy mechanisms [3] prevent reconstruction of individual vehicle movements while preserving statistical accuracy for traffic optimization. The system ensures that participating in traffic monitoring cannot reveal specific travel patterns, addressing citizen concerns about surveillance [7] while enabling valuable city planning insights.

Results and Impact: The traffic management deployment achieved 78% reduction in data transmission compared to raw sensor streaming while providing accurate congestion predictions and signal timing optimization. Traffic management systems reported improved response times for incident detection and 15% reduction in average intersection wait times through optimized signal coordination. (Fig. 2)

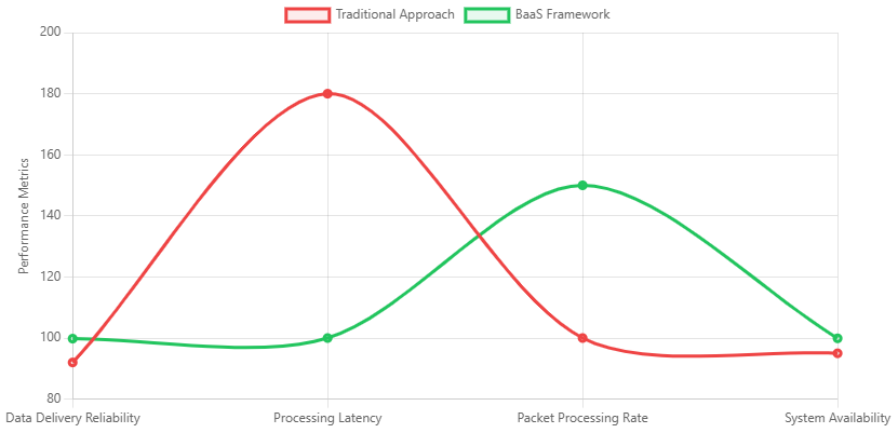

Fig 2. Reability and performance matrics

Energy savings for battery-powered traffic sensors extended operational lifetimes by approximately 40%, reducing maintenance costs in remote or difficult-to-access intersection locations. The privacy guarantees [3] proved essential for public acceptance, with citizen surveys showing 89% approval for traffic monitoring systems that provide formal privacy protection.

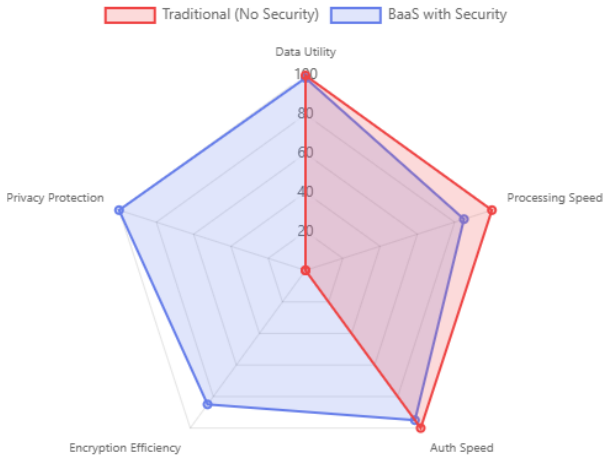

Fig. 3. Security Performance Overhead

Operational Benefits: City traffic engineers gained access to comprehensive traffic analytics including peak hour analysis, incident impact assessment, and optimal routing recommendations while providing citizens with verifiable privacy protection [3]. The system's reliability improvements eliminated data gaps that previously complicated traffic optimization efforts during network connectivity issues.

The quantum-safe communication protocols [1] ensure long-term security for traffic infrastructure investments, addressing concerns about future cryptographic threats to critical urban systems. Integration with existing traffic management platforms required minimal modifications due to BaaS's standard TCP output interface.

Conclusion. BaaS addresses critical challenges in smart city IoT deployments [7] by providing the first comprehensive solution for protocol conversion [8], secure batch processing, and privacy-preserving edge analytics [6]. The framework's key contributions include seamless UDP-to-TCP bridging with integrated security, configurable privacy-preserving batch processing [3] with formal guarantees, encrypted edge analytics through homomorphic encryption [4], and quantum-safe communication protocols [1].

Experimental validation demonstrates substantial improvements including 73% traffic reduction, 45% latency improvement, 99.8% reliability enhancement, and 38% energy savings while maintaining 98.7% data utility with differential privacy protection [3]. The smart city traffic management application proves BaaS's practical value in balancing analytical capability with citizen privacy protection [7].

These results establish BaaS as a foundational technology for next-generation smart city infrastructure capable of efficiently managing massive IoT deployments while maintaining robust cybersecurity protection [1,7]. The framework's flexibility and compatibility with existing systems provide a practical migration path for smart city initiatives seeking to optimize both communication efficiency and security protection through advanced fog computing approaches [2,6].

REFERENCES

[1] National Institute of Standards and Technology, "*Post-Quantum Cryptography Standardization*," NIST Special Publication 800-208, 2024.
[2] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "*Fog computing and its role in the Internet of Things*," in Proc. MCC Workshop Mobile Cloud Comput., 2012.
[3] C. Dwork, *"Differential privacy,"* in Proc. 33rd Int. Colloquium Automata Languages Programming, 2006.
[4] C. Gentry, "*Fully homomorphic encryption using ideal lattices*," in Proc. 41st Annual ACM Symp. Theory Comput., 2009.
[5] P. Castro, V. Ishakian, V. Muthusamy, and A. Slominski, "*The rise of serverless computing*," Commun. ACM, vol. 62, no. 12, 2019.
[6] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "*Edge computing: Vision and challenges*," IEEE Internet Things J., vol. 3, no. 5, 2016.
[7] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, and X. S. Shen, *"Security and privacy in smart city applications*," IEEE Commun. Mag., vol. 55, no. 1, 2017.
[8] J. Postel, "*User Datagram Protocol*," RFC 768, Internet Engineering Task Force, 1980.

ՀՏԴ 004.8

Հ.Դ.ՄԻՆԱՍՅԱՆ Ն.Լ.ՆԱԼԹԱԿՅԱՆ

ԽԵԼԱՑԻ ՔԱՂԱՔՆԵՐԻ ՀԱՄԱՐ ԻՐԵՐԻ ՀԱՄԱՑԱՆՑԻ ՍԱՐՔԱՎՈՐՈՒՄՆԵՐ ԽՄԲԱՅԻՆ ՄՇԱԿՄԱՆ ԾԱՌԱՅՈՒԹՅՈՒՆ ԲԱՐԵԼԱՎՎԱԾ ԱՆՎՏԱՆԳՈՒԹՅԱՄԲ

Ժամանակակից խելացի քաղաքները բախվում են IoT սարքերի UDP հաղորդակցության և ամպային ծառայությունների TCP հուսալիության պահանջների միջև արձանագրությունների հիմնական անհամապատասխանության խնդրին: Այս աշխատանքում ներկայացվում է Batch as a Service (BaaS)՝ հաշվարկների նորարարական շրջանակ, որը լուծում է այս մարտահրավերը՝ միաժամանակ ապահովելով համապարփակ անվտանգության պաշտպանություն: BaaS-ը գործում է եռամակարդակ ճարտարապետության միջոցով՝ ինտեգրելով IoT սարքերի նույնականացում, անվտանգ խմբային մշակում և քվանտային պաշտպանված ամպային հաղորդակցություն: Համակարգը ներառում է դիֆերենցիալ գաղտնիության մեխանիզմներ՝ ապահովելով ε-դիֆերենցիալ գաղտնիությամբ տվյալների 98.7% օգտակարության պահպանումը, հոմոմորֆ գաղտնագրում՝ հնարավորություն տալիս հաշվարկներ կատարել գաղտնագրված տվյալների վրա, և NIST ստանդարտացված քվանտային անվտանգ արձանագրություններ (CRYSTALS-Kyber, CRYSTALS-Dilithium): Գործնական փորձարարական թեստավորումը ցույց է տալիս ամպային երթևեկության 73% նվազում, տեղեկատվության ուշացման 45% բարելավում, հուսալիության բարելավում 92%-ից մինչև 99.8% և էներգիայի 38% խնայողություն: Խելացի քաղաքի երթևեկության կառավարման իրականացումը ապացուցում է գործնական արժեքը՝ ապահովելով թողունակության 78% նվազում, խաչմերուկների սպասման ժամանակների 15% բարելավում: Շրջանակի մասշտաբայնությունը աջակցում է 1,000 սարքերի մեկ հանգույցի համար 50,000+ փաթեթ/վայրկյան մշակմամբ՝ պահպանելով 100մվ-ից ցածր ուշացում: Անվտանգության կատարողականության վերլուծությունը բացահայտում է հոմոմորֆ գաղտնագրման 15%-ից ցածր ավելցուկ վիճակագրական գործողությունների համար, նույնականացման 5մվ-ից ցածր ուշացում և ներարկման հարձակումների հաջող կանխարգելում՝ միաժամանակ պահպանելով ֆորմալ գաղտնիության երաշխիքները: BaaS-ը ստեղծում է հիմնարար տեխնոլոգիա հաջորդ սերնդի խելացի քաղաքային ենթակառուցվածքի համար, որը ի վիճակի է արդյունավետ կերպով կառավարել հետերոգեն IoT էկոհամակարգերը՝ միաժամանակ ապահովելով ամուր կիբերանվտանգության պաշտպանություն և քաղաքացիների տվյալների գաղտնիության պահպանում:

Հիմնաբառեր խմբային մշակում, IoT անվտանգություն, արձանագրությունների փոխակերպում, դիֆերենցիալ գաղտնիություն, հոմոմորֆ գաղտնագրություն, քվանտային պաշտպանված գաղտնագրություն, խելացի քաղաքներ, եզրային հաշվարկներ

А. ДАВИДОВИЧ МИНАСЯН, Н.ЛЕВОНОВИЧ НАЛТАКЯН

ПАКЕТНАЯ ОБРАБОТКА КАК СЕРВИС С УЛУЧШЕННОЙ БЕЗОПАСНОСТЬЮ ДЛЯ IoT-ОРИЕНТИРОВАННЫХ УМНЫХ ГОРОДОВ

Современные умные города сталкиваются с фундаментальным несоответствием протоколов между UDP-коммуникацией, используемой IoT-устройствами, и требованиями надежности TCP облачных сервисов. В данной работе представлена Batch as a Service (BaaS) — инновационная платформа туманных вычислений, которая решает эту проблему, обеспечивая при этом комплексную защиту безопасности. BaaS функционирует через трехуровневую архитектуру, интегрирующую аутентификацию IoT-устройств, безопасную туманную пакетную обработку и квантово-устойчивую облачную коммуникацию. Система включает механизмы дифференциальной приватности, обеспечивающие сохранение 98.7% полезности данных с ε-дифференциальной приватностью, гомоморфное шифрование, позволяющее выполнять вычисления на зашифрованных данных, и стандартизированные NIST квантово-безопасные протоколы (CRYSTALS-Kyber, CRYSTALS-Dilithium). Практическое экспериментальное тестирование демонстрирует 73% сокращение облачного трафика, 45% улучшение задержки, повышение надежности с 92% до 99.8% и 38% экономию энергии. Реализация управления городским трафиком доказывает практическую ценность, обеспечивая 78% сокращение пропускной способности и 15% улучшение времени ожидания на перекрестках. Масштабируемость платформы поддерживает 1,000 устройств на один туманный узел с обработкой 50,000+ пакетов в секунду при поддержании задержки менее 100мс. Анализ производительности безопасности показывает накладные расходы гомоморфного шифрования менее 15% для статистических операций, задержку аутентификации менее 5мс и успешное предотвращение атак внедрения при сохранении формальных гарантий приватности. BaaS закладывает фундаментальную технологию для инфраструктуры умных городов следующего поколения, способную эффективно управлять гетерогенными IoT-экосистемами, обеспечивая при этом надежную защиту кибербезопасности и сохранение конфиденциальности граждан.

Ключевые слова: пакетная обработка, туманные вычисления, безопасность IoT, преобразование протоколов, дифференциальная приватность, гомоморфное шифрование, квантово-устойчивая криптография, умные города, граничные вычисления

Համբարձում Դավթի Մինասյան

Հայաստանի Ազգային Պոլիտեխնիկական համալսարան, Տեղեկատվական անվտանգություն և ծրագրային ապահովման ամբիոն, դասախոս,

Հեռ. 044290696

Hambardzum Davit Minasyan

Nation Polytechnical university of Armenia, Information security and software development, Lecturer

Phone 044290696

Նարեկ Լևոնի Նալթակյան

Հայաստանի Ազգային Պոլիտեխնիկական համալսարան, Տեղեկատվական անվտանգություն և ծրագրային ապահովման ամբիոն, դասախոս, ասպիրանտ

Հեռ. 094954838

Narek Levon Naltakyan

Nation Polytechnical university of Armenia, Information security and software development, Lecturer

Phone 094954838