UDC 004.7
DOI: 10.53297/18293336-2025.2-70

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

H.D. Minasyan, N.L. Naltakyan

National Polytechnic University of Armenia

Smart cities of modern day have a huge problem since most IoT devices use a UDP communication that is fast but not reliable and cloud services use TCP that is slower but reliable. In this paper, Batch as a Service (BaaS), a fog computing system that solves the problem of not being suitable while adding good protection of security. BaaS uses a three-layer design that unites the authentication of IoT devices, secure processing of fog-based batches, and communication with the cloud that is also secured. The system uses differential privacy keeping the data almost fully usable at 98.7% with ε-differential privacy, homomorphic encryption so calculations can happen on the encrypted data, and NIST-standardized quantum-safe protocols (CRYSTALS-Kyber, CRYSTALS-Dilithium). Experiments show that the system makes cloud traffic lower for 73%, cuts latency by 45%, raises reliability from 92% to 99.8%, and saves energy for 38%. In the test of the traffic in smart cities it lowers the use of bandwidth by 78% and has 15% of intersection waiting times upgraded. The system grows well, and it can use around 1,000 devices for each fog node and can process more than 50,000 packets in a second while latency being sub-100 *ms*. Security tests show the extra cost of homomorphic encryption is below 15% for basic operations of statistics, authentication latency is under 5 *ms*, and the system can put a stop to the injection attacks while keeping strong guarantees of privacy. BaaS sets fundamental technology for future smart cities helping the cities in managing all the IoT devices efficiently but also having the privacy of both citizen and security protected.

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

Introduction. A huge number of IoT devices in smart cities cause a big problem in communication [1]. Resource-constrained devices prefer using UDP protocols [2] because it is simple while cloud services expect the reliability of TCP. With 75 billion number of devices that are expected by 2025 producing 530% more data than traditional system, the mismatch of this protocol creates problems in both efficiency and security. The latest analysis shows that IoT-targeted attacks go up by 124%, which makes security integration essential for smart city deployments [1].

In this paper, Batch as a Service (BaaS), a full fog computing system [3] that combines protocol conversion with strong security is introduced. BaaS collects UDP packets [2] from many IoT devices, provides batch processing while protecting the data, and sends the results to the cloud through quantum-safe TCP connections [4,5]. The strongest point of the system is that security and efficiency are built together from the very beginning instead or being added later.

The system design. BaaS uses a three-layer hierarchical architecture (Fig. 1) that fits well with smart city system [1] while addressing security needs that come with handling the sensitive citizen data. The idea of the design is focused on combining protocol-aware security, privacy protection and communication efficiency so they would support each other.

Fig. 1. System Design

The IoT Device Layer has simple UDP communication [2] and just basic authentication to keep the security without having limited resources in a heavy load. The BaaS Fog Layer is taken over by the Secure Batch Manager, which gathers the UDP reception that soon will be received, groups them with methods that keep privacy and forms batches dependent on time duration, size of data, or conditions of events. At the Cloud Layer those batches that are encoded are sent over to TCP connections which are trustworthy, handing over the data that is cloud secure while having bandwidth saved as well.

Technical innovations. UDP-to-TCP transformation [2] and strong features of security can be united by BaaS that has the authentication of the device, batch processing, which is secured, and aggregation that has a strong privacy. This can be useful in solving the issue of having heterogeneous protocol environments protected in the smart cities [1]. Privacy-Preserving Batch Processing: During aggregation the system uses differential privacy [6], making sure individual device contributions cannot be revealed from the results of batch. The privacy mechanism satisfies:

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

M is the privacy mechanism, D and D' are datasets differing by one individual, and ε takes over privacy strength [6]. 98.7% of data performance is maintained with ε = 1.0.

Computation on data that is encoded is allowed by BaaS without decryption through serverless computing features that are built-in [7]. For encrypted values c_1, c_2, the homomorphic property allows:

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

Analyzing data, detecting anomaly, and transforming data securely with the confidentiality of the information during processing are made possible by this [8].

Quantum-Safe communication. NIST-standardized post-quantum protocols [5] are used by the system (CRYSTALS-Kyber, CRYSTALS-Dilithium) with hybrid key formation:

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

So it makes sure there is good protection from current and also future quantum computing dangers while still working with existing systems. [5].

Experimental. Raspberry Pi 4 fog nodes were used during the testing of BaaS which use data from artificial IoT sensors across three smart city cases: tracking the conditions of the environment (low in frequency), metadata of video analytics (medium in frequency), and industrial sensors (high in frequency). Each of the cases tested different activities in network and demands that are like the conditions of real smart city that rely on edge computing [4].

Results. Effectiveness of Communication: In the BaaS system there is a cut of traffic for 73% which is sent to the cloud. The batches are combined well when we compare them with single transfers of UDP [8]. The reduction of the latency is 45% and this is a result of better operating of batches and transfers of TCP. It also removes delays that are caused by UDP packets.

Improved Reliability: BaaS protocol converting and grouping of batches had reliability of data delivery go up from 92% with direct UDP [2] to 99.8%. The improvement where losing data can have a big effect on critical services is very important for smart city system [1].

Better Energy Management: IoT devices have reduced energy by 38% and this is thanks to be removing the packet transfers and the system load. The device has longer operation in edge computing which is for sensors that have a battery [4].

Security Effectiveness: The private data value is 98.7% and the rules of privacy for individual data are applied [7]. Additional 15% of processing was added using homomorphic encryption [8]. This shows the latency, that is under 5 ms, while making the entry of data that is not proved to stop.

Scalability: 1,000 IoT devices can be operated by any fog node at the same time with more than 50,000 packets in a second. Less 100 *ms* can take for batch operation with 99.9% rates of success and from 100 to 200 packets have the data that is sent in batches and because of this latency and performance are in balance. So, there is better growth in the environments of local computing [4].

Smart city traffic management system. In traffic monitoring, the use of BaaS shows that the system makes full analytics and the importance of keeping citizen's information private equal [1]. In our experiment we worked on data that came from 400 intersections. Also, we followed things like vehicle counts, speed, and traffic movement all over the city.

Traffic systems have a huge problem in making sure that cities need data to manage traffic, but they don't want to follow individual vehicles [1]. The methods that exist either risk privacy by tracking vehicles thoroughly or lose useful information because there is more data combined.

BaaS has managed a solution to this problem. It uses its batch processing to keep data private [7]. It gathers real-time traffic information by using UDP [2] from different intersections, uses privacy mechanisms [7] during fog-based gathering, and sends summaries of statistics to traffic managing systems in each 5 minutes.

Operational details. In every 10 seconds the number of vehicles and information about speed is sent through intersection devices using UDP[2]. The data is collected by BaaS fog nodes from 20-30 intersections nearby and it calculates the statistics of traffic with differential privacy [7] for protection adding carefully controlled noise. If there is a case of heavy traffic or an accident, the system alerts immediately but still have protected privacy.

Privacy Protection. Rebuilding of car movements can be stopped by differential methods of privacy [7] but keeping correct statistics for traffic improvement. It makes sure that taking part in traffic monitoring doesn't mean that travel patterns can be exposed. The system secures privacy. At the same time, it gives useful information for improving traffic and road loads [1].

Results and Impact. Data use was reduced by 78% from traffic management if we compared to sending original information of sensor. But it still has reliable predictions of traffic jams to improve the timing of traffic lights. There are some improvements made by the system if there is something wrong in the duration of

response. The waiting time for meeting points dropped by 15% because of better organized signals (Fig. 2).

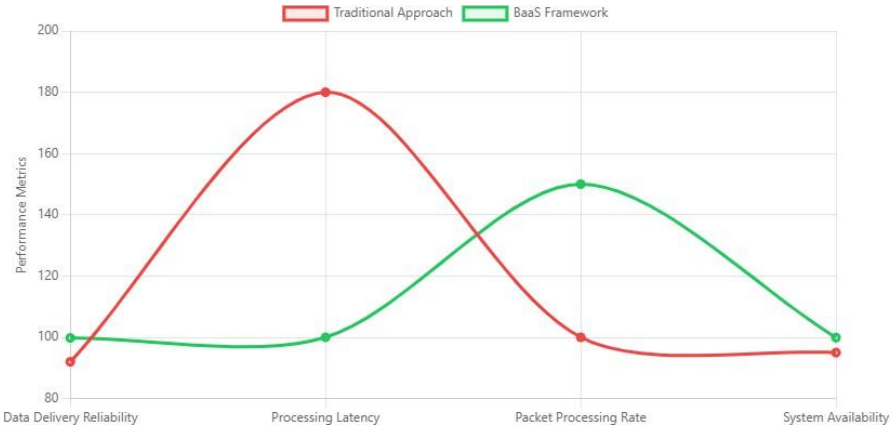

Fig. 2..Reability and performance matrics

The new system had improvements for traffic sensors that are powered by battery to last around 40% longer, which causes less maintenance work in remote or intersection locations that are difficult to reach. Rules of privacy [7] also had great importance for people. The system of traffic monitoring that has a protection of privacy was supported by about 89% of citizens.

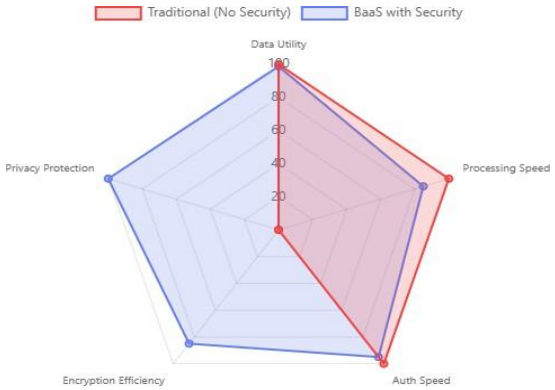

Fig. 3. Security performance overhead

Operational benefits. The engineers of traffic now have access to the traffic data which includes the data of peak hour, accidents effect on the movement, and suggestions for better routing while having citizens provided with protection of privacy [7]. The improvements in the system's reliability have removed data gaps

that are used to make difficulties in planning the complicated traffic when networks have some problems.

The system of the traffic is protected by quantum-safe communication protocols [5] from future concerns in security so that the city's infrastructure investments remain safe. When working with traffic management platforms, minimal modifications are needed due to BaaS's standard TCP output interface.

Conclusion. Major problems of IoT deployments in smart cities can be solved by BaaS [1] which offers solutions for converting protocol [2], processing of batch securely, and edge analytics that maintain privacy [4]. The system has strong points in smooth UDP-to-TCP conversion that has strong built-in security, batch processing with protected privacy [7] with formal guarantees, encrypted analytics using homomorphic encryption [8], and protocols of quantum-safe communication [5].

Experiments show great improvements which consist of 73% cut in traffic, 45% better latency, 99.8% higher reliability, and 38% savings in energy but keeping 98.7% of data with differential protection of privacy [7]. The traffic management in smart cities proves that BaaS can support analytics while still having the citizens' privacy protected [1].

According to these results, BaaS is a foundational technology for future smart city systems. It can efficiently manage big IoT deploy flexibility of the system, which makes it easy to provide a practical migration path for smart city while having both communication efficiency and security protection improved through developed fog computing methods [3,4]

References

1. Security and privacy in smart city applications / **K. Zhang, J. Ni, K. Yang, X. Liang et al //** IEEE Commun. Mag., Vol. 55, no. 1.- 2017.- P. 122-129.
2. **Postel J.,** "User Datagram Protocol,"RFC768, Internet Engineering Task Force, 1980.
3. **Bonomi F., Milito R., Zhu J., and Addepalli S.** Fog computing and its role in the Internet of Things // Proc. MCC Workshop Mobile Cloud Comput.- 2012.- P. 13-16.
4. **Shi W., Cao J., Zhang Q., Li Y., and Xu L.** Edge computing: Vision and challenges // IEEE Internet Things J., Vol. 3, no. 5.- 2016.- P. 637-646.
5. National Institute of Standards and Technology, "Post-Quantum Cryptography Standardization"- NIST Special Publication 800-208, 2024.
6. **Dwork C.** Differential privacy // Proc. 33rd Int. Colloquium Automata Languages Programming.- 2006.- P. 1-12.
7. **Castro P., Ishakian V., Muthusamy V., and Slominski A.** The rise of serverless computing // Commun. ACM.- 2019.- Vol. 62, no. 12.- P. 44-54.
8. **Gentry C.** Fully homomorphic encryption using ideal lattices // Proc. 41st Annual ACM Symp. Theory Comput.- 2009.- P. 169-178.

Received on 26.11.2025.
Accepted for the publication on 29.01.2026.

ԽԵԼԱՑԻ ՔԱՂԱՔՆԵՐԻ ՀԱՄԱՐ ԻՐԵՐԻ ՀԱՄԱՑԱՆՑԻ ՍԱՐՔԱՎՈՐՈՒՄՆԵՐ ԽՄԲԱՅԻՆ ՄՇԱԿՄԱՆ ԾԱՌԱՅՈՒԹՅՈՒՆ ԲԱՐԵԼԱՎՎԱԾ ԱՆՎՏԱՆԳՈՒԹՅԱՄԲ

Հ.Դ. Մինասյան, Ն.Լ.Նալթակյան

Ժամանակակից խելացի քաղաքները բախվում են լուրջ խնդիրների, քանի որ շատ IoT սարքեր օգտագործում են UDP հաղորդակցության ծառայությունը, որը արագ է, բայց ոչ այդքան հուսալի, և TCP ամպային ծառայությունը, որը ավելի դանդաղ է, բայց հուսալի: Այս աշխատանքում ներկայացվում է Batch as a Service (BaaS)՝ հաշվարկների նորարարական շրջանակ, որը լուծում է հուսալիության խնդիրը՝ միաժամանակ ապահովելով անվտանգության պաշտպանություն: BaaS-ը օգտագործում է եռամակարդակ ճարտարապետություն, որն ինտեգրում է IoT սարքերի նույնականացումը, անվտանգ խմբային մշակումը և քվանտային պաշտպանված ամպային հաղորդակցությունը: Համակարգը կիրառում է դիֆերենցիալ գաղտնիության մեխանիզմներ՝ ապահովելով ε-դիֆերենցիալ գաղտնիությամբ տվյալների օգտակարության պահպանումը գրեթե ամբողջությամբ՝ 98.7%-ով, հոմոմորֆ գաղտնագրում՝ հնարավորություն տալով, որ հաշվարկները կատարվեն գաղտնագրված տվյալների վրա, և NIST ստանդարտացված քվանտային անվտանգ արձանագրություններ (CRYSTALS- Kyber, CRYSTALS-Dilithium): Գործնական թեստավորումը ցույց է տալիս, որ ամպային երթևեկությունը 73%-ով նվազել է, տեղեկատվության ուշացումը 45%-ով բարելավվել է, հուսալիությունը աճել է 92%-ից մինչև 99.8%, իսկ էներգիայի խնայողությունը՝ 38%: Խելացի քաղաքի երթևեկության կառավարման իրականացման գործնական արժեքն ապահովում է թողունակության 78% նվազում, խաչմերուկների սպասման ժամանակների 15% բարելավում: Շրջանակի մասշտաբայնությունն աջակցում է 1,000 սարքերի մեկ հանգույցին և կարող է մշակել ավելի քան 50,000 փաթեթ մեկ վայրկյանում ՝ պահպանելով 100մվ-ից ցածր ուշացում: Անվտանգության կատարողականության վերլուծությունը բացահայտում է հոմոմորֆ գաղտնագրման 15%-ից ցածր ավելցուկ վիճակագրական գործողությունների դեպքում, նույնականացման 5 մվ-ից ցածր ուշացում և ներարկման հարձակումների հաջող կանխարգելում՝ միաժամանակ պահպանելով ֆորմալ գաղտնիության երաշխիքները: BaaS-ը ստեղծում է հիմնարար տեխնոլոգիա ապագա խելացի քաղաքային ենթակառուցվածքի համար, որն օգնում է արդյունավետ կերպով կառավարել հետերոգեն IoT էկոհամակարգերը՝ միաժամանակ ապահովելով ամուր պաշտպանություն և քաղաքացիների տվյալների գաղտնիության պահպանում:

Առանցքային բառեր. խմբային մշակում, IoT անվտանգություն, արձանագրությունների փոխակերպում, ամպային հաշվարկներ, դիֆերենցիալ գաղտնիություն, հոմոմորֆ գաղտնագրություն, քվանտային պաշտպանված գաղտնագրություն, խելացի քաղաքներ, եզրային հաշվարկներ:

ПАКЕТНЫЙ СЕРВИС С УЛУЧШЕННОЙ БЕЗОПАСНОСТЬЮ ДЛЯ IoT-ОРИЕНТИРОВАННЫХ УМНЫХ ГОРОДОВ

А.Д. Минасян, Н.Л. Налтакян

Современные умные города сталкиваются с серьезными проблемами, поскольку многие устройства Интернета вещей используют протокол UDP, который быстр, но не так надежен, и облачный протокол TCP, который медленнее, но надежен. В данной работе представлена Batch as a Service (BaaS) - инновационная вычислительная платформа, которая решает проблему надежности, обеспечивая при этом защиту безопасности. BaaS использует трехслойную архитектуру, которая интегрирует аутентификацию устройств Интернета вещей, безопасную пакетную обработку и квантово-защищенную облачную связь. Система использует дифференциальные механизмы конфиденциальности, гарантирующие практически полное сохранение целостности данных с ε-дифференциальной конфиденциальностью 98,7%, гомоморфное шифрование, позволяющее выполнять вычисления с зашифрованными данными, и стандартизированные NIST квантово-безопасные протоколы (CRYSTALS-Kyber, CRYSTALS-Dilithium). Практические испытания показывают, что облачный трафик сокращается на 73%, задержка информации улучшается на 45%, надежность увеличивается с 92% до 99,8%, а экономия энергии составляет 38%. Практическая ценность внедрения интеллектуального управления дорожным движением в городе заключается в снижении пропускной способности на 78% и уменьшении времени ожидания на перекрёстках на 15%. Масштабируемость платформы позволяет использовать 1000 устройств на узел и обрабатывать более 50 000 пакетов в секунду, сохраняя при этом задержку менее 100 *мс*. Анализ эффективности безопасности показывает гомоморфную избыточность шифрования менее 15% для статистических операций, задержку менее 5 *мс* для аутентификации и успешное предотвращение атак с внедрением данных при сохранении формальных гарантий конфиденциальности. BaaS создаёт основополагающую технологию для будущей инфраструктуры интеллектуального города, которая помогает эффективно управлять гетерогенными экосистемами Интернета вещей, обеспечивая при этом надёжную защиту и сохраняя конфиденциальность данных граждан.

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