
دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران

**بررسی مقاله سوم درس معماری پیشرفته سیستم های کامپیوتری**

# RDIC: A blockchain-based remote data integrity checking scheme for IoT in ٥G networks

# طرح بررسی یکپارچگی داده از راه دور مبتنی بر بلاکچین برای اینترنت اشیا در شبکه های G۵

**دانشجو:**

**محمد زکریا دهقانی**

**استاد راهنما:**

**دکتر جاسبی**

**بهار ۱۴۰۰**

**فهرست مطالب**

**عنوان** **صفحه**

# تعریف مسئله و هدف اصلی مقاله

## ۱–۱- سوال اصلی مطرح شده در مقاله

یکی از اصلی ترین کاربرد شبکه های همراه نسل ۵[۱] ،اینترنت اشیا (IoT) است. با توسعه سریع شبکه G۵ ، دستگاه های ترمینال اینترنت اشیا داده های بزرگی ایجاد کرده اند. همچنین دستگاه های متصل به اینترنت اشیا باید سبک بوده و از نگهداری حجم زیادی از داده اجتناب کنند ، به عنوان مثال ،در دستگاه های پوشیدنی[۲]. حجم داده زیادی از اطلاعاتی که فرد در موقعیت آن قرار دارد تولید می شود که جهت استفاده کاربردی از آن بهترین راه استفاده از فضای ابری جهت نگهداری داده ها می باشد. با توجه به اینکه فضای ابری از کنترل کاربر خارج است، قابلیت اطمینان و امنیت داده از اهمیت بالایی برخوردار است.همچنین یکپارچگی داده های جمع آوری شده از راه دور از اهمیت بالایی برخوردار است که در این طرح یک روش یکپارچگی داده[۳] از راه دور مبتنی بر بلاکچین[۴] برای داده های بزرگ دراینترنت اشیا ارائه شده است.

در این طرح مفهوم جدیدی از تکنیک بلاکچین معرفی می شود که کارایی و امنیت را بهبود می بخشد. در نهایت با به کار بردن امضای دیجیتالی RSA و بلاکچین ، امنیت و کارایی این سیستم بررسی می شود.

## ۱–۲- چالش مسئله

با استفاده از فناوری ارتباطات پر سرعت موبایل g ۵ ، اینترنت اشیا می تواند جهان فیزیکی و اشیا مجازی را به هم پیوند دهد. اینترنت اشیا را می توان در زمینه های تجاری و امنیت هوشمند استفاده کرد. مثالی از این کاربردها می تواند شهرهای هوشمند ، کارخانه های هوشمند و میدان جنگ هوشمند باشد. در زمان جمع آوری اطلاعات فرآهم شده در این بسترها ، چالش اصلی یکپارچگی و امنیت و احراز هویت ارسال کننده داده می باشد.

---

[۱] ۵G

[۲] wearable devices

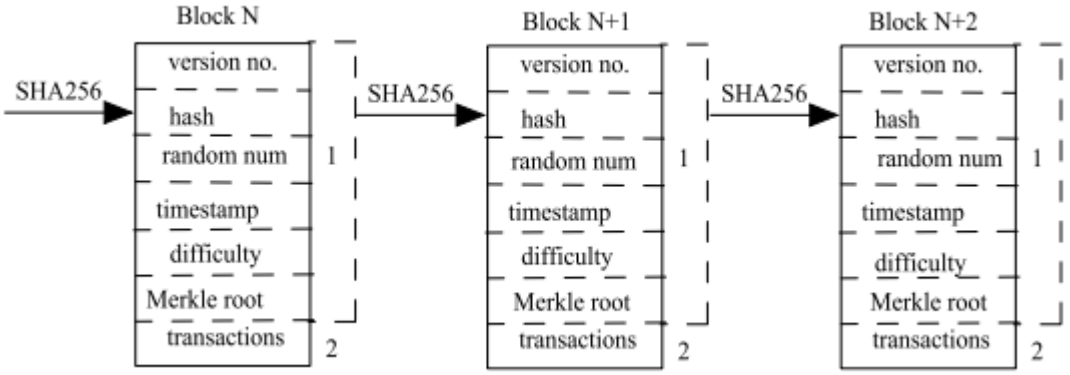
[۳] data integrity

[۴] blockchain

زمانی که این اطلاعات در بستر ابری بارگزاری می شود چک کردن اتمام بارگزاری و صحت اطلاعات از اهمیت بالایی برخوردار است. همچنین طرحی که بتواند به سادگی بر روی تمام دستگاه های اینترنت اشیا پیاده سازی شود از چالش های اصلی می باشد.

## ۱–۳- ضرورت حل مسئله

بلاکچین به عنوان یک دفتر توزیع شده دارای ویژگی های تمرکززدایی[۱] ، عدم دستکاری[۲] ، فضای ذخیره سازی توزیع شده[۳] می باشد. برای اولین بار فناوری بلاک چین در رمز ارزها به کار برده شده است. هر بلاک شامل یک عدد است[۴] که با محاسبه این عدد به یک hash واحد در بلوک ها می رسیم. کلیه بلوک های متصل به شبکه با محاسبه این hash به صورت زنجیره وار با یکدیگر ارتباط دارند. در این زنجیره با تغییر hash محاسبه شده از بلوک قبلی می توان به تغییر اطلاعات در جریان زنجیره پی برد. معماری زنجیره بلوک ها به صورت شکل ۱ می باشد.




**شکل ۱ – زنجیره بلوک ها**

به عنوان مثال در رمز ارز bitcoin از الگوریتم sha۲۵٦ استفاده شده است. از این روش می توان در احراز هویت و صحت سنجی اطلاعات شبکه اینترنت اشیا استفاده کرد. اساس طرح پیشنهادی هم بر همین روش استوار است.

---

۱ decentralization

۲ non-tamperability

۳ distributed storage

۴ nonce

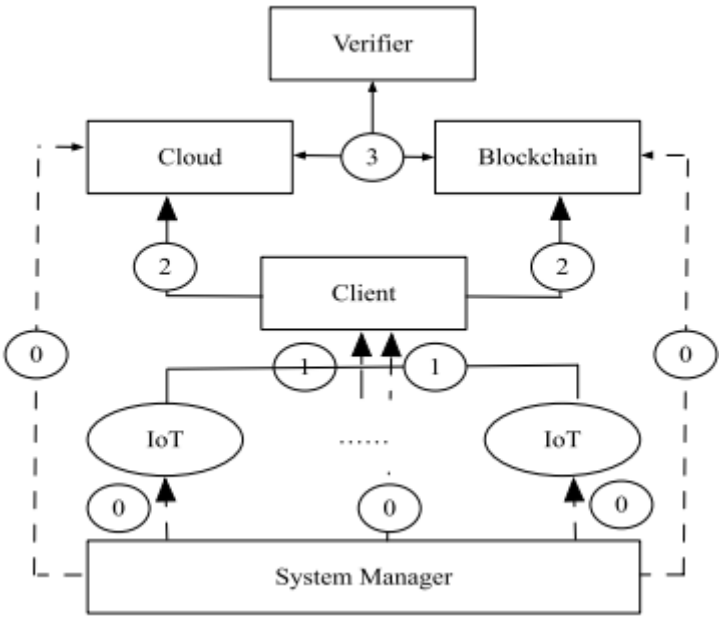
## ۱-۴- کارهای قبلی انجام شده

در سال ۲۰۰۸ زنجیره بلوک ها توسط ناکاموتو برای رمز ارز بیت کوین استفاده شد. به منظور رسیدن به ویژگی های عدم دستکاری و صحت اطلاعات در بلاکچین از برخی از ابزارهای رمزنگاری مانند تابع hash ، امضای دیجیتال و درخت Merkle hash استفاده می شود. در [۱] یک روش برای انتقال اطلاعات به صورت امن که از تابع hash استفاده می کند ارائه شده است. در شبیه سازی انجام شده، بازدهی این رمز ارزها در دنیای واقعی بررسی شده است. در [۲] نشان داده شده که می توان به اطلاعات هویتی افرادی که بیت کوین را منتقل می کنند پی برد، در صورتی که ویژگی اصلی رمز ارز ها ناشناس ماندن طرفین معامله می باشد. از زمان ظهور این فن آوری ، رمز ارز های مختلف برای کاربردهای مختلفی پیشنهاد شده است. به عنوان مثال در سال ۲۰۲۱ رمزارزهای mixcoin و مونیرو برای استفاده در شبکه حمل و نقل عمومی پیشنهاد شده است [۳] . حافظت از اطلاعات شخصی همواره یکی از مهمترین مباحث تراکنش های مالی بوده که زنجیره بلوک ها می تواند این اطمینان از حفاظت داده را فرآهم کند. زنجیره بلوک ها علاوه بر استفاده در رمز ارزها می تواند در امنیت شبکه و یا فرآیندهایی مثل گزارش های ناشناس هم مورد استفاده قرار گیرد [۴]. همچنین پروتکل های سلسله مراتبی بر مبنای زنجیره بلوک برای شبکه هم در[۵] پیشنهاد شده است.در [۶] یک مطالعه تحقیقاتی در حوزه امنیت شبکه های هوشمند با استفاده از زنجیره بلوک ها انجام شده است.

برای بهبود تاثیر روش های کنترل یکپارچگی داده با استفاده از زنجیره بلوک ها روش های زیادی پیشنهاد شده است. از جمله در روش [۷] با داشتن اطلاعات خصوصی مبتنی بر بلاکچین کارایی را به طور چشمگیری بهبود می بخشد.

## ۱–۵- روش ارائه شده در مقاله اصلی

پیاده سازی این روش شامل ۴ مرحله راه اندازی – جمع آوری داده – بارگزاری داده – صحت اطلاعات می باشد:




**شکل ۲ معماری روش RDIC**

مرحله اول : در مرحله اول قسمت هایی که با عدد ۰ مشخص شده اند فاز راه اندازی این روش می باشد. مدیر سیستم پارامترهای محاسبات را مقداردهی می کند و در همین زمان اطلاعات توسط اینترنت اشیا تولید شده می شود.

مرحله دوم: در مرحله دوم که با عدد ۱ مشخص شده فاز جمع آوری اطلاعات است که دستگاه های اینترنت اشیا داده های خود را برای ایستگاه های کاری ارسال می کنند.

مرحله سوم: در مرحله سوم که با عدد ۲ نشان داده شده فاز بارگزاری اطلاعات است. در این مرحله ایستگاه های کاری داده ها را دسته بندی و پردازش می کنند و جهت ارسال به فضای ابری با استفاده از زنجیره بلوک ها آماده می کنند.

مرحله چهارم : در این مرحله که با عدد ۳ نمایش داده شده فاز صحت سنجی اطلاعات بوده که با استفاده از محاسبات انجام شده از طریق زنجیره بلوک صحت یکپارچگی داده ها در این مرحله بررسی و تایید می شود.

# فصل ۲-  راه حل پیشنهادی برای حل مسئله

برای پیاده سازی این روش به صورت تئوری چهار مرحله زیر پیاده سازی شده است:

مرحله اول راه اندازی اولیه:

فرض کنیم N تعداد ماژول هایی که داده تولید می کنند باشد. در این صورت با دو فاکتور عدد اول p و q میتوان رابطه N=pq را در نظر گرفت.

$p = ۲p' + ۱$

$q = ۲q' + ۱$

طبق رابطه اویلر : $\phi(N) = (p-۱)(q-۱)$

اگر l مقدار فضایی که جهت محاسبات نیاز است باشد: $n = |F|/l$ که $|F|$ برابر تعداد بیت های F است.

تابع تصادفی: $f : Z^* N \times \{۱, ۲, \ldots, n\} \rightarrow Z^* N$

تابع تصادفی جایگشتی : $\pi : Z^*N \times \{1, 2, \ldots, n\} \rightarrow \{1, 2, \ldots, n\}$

مرحله دوم جمع آوری داده ها:

بر اساس نیاز ایستگاه های کاری دستگاه های متصل به شبکه اینترنت اشیا داده های خود را به این ایستگاه ها ارسال می کنند. فرض کنیم Mi داده از اشیای موجود در شبکه جمع آوری شده است.

$Mi = Esk(M^-i)$ تابع داده های رمز شده می باشد که این داده رمز شده به ایستگاه های کاری ارسال می شود.

مرحله سوم بارگزاری داده ها:

فرض کنیم داده های رمز شده mi تا mn در ایتسگاه های کاری دریافت شده اند. ایستگاه این داده ها را با sk رمز گشایی می کند.

تابع داده های رمزگشایی شده : $M^-i = Dsk(Mi)$

از اینجا به بعد هر ایستگاه کاری مراحل زیر را دنبال می کند:

- تقسیم داده ها به بخش های کوچکتر $n = \lceil |F|/l \rceil$ and $۲l \gg \phi(N)$
- محاصبه fi به ازای هر بلوک داده $fi = Fi \bmod \phi(N)$
- تولید امضای دیجیتال به ازای هر بلوک داده $h = H(F)$
- بارگزاری بلوک شماره n به همراه عدد hash محاسبه شده در فضای ابری به همراه امضای دیجیتال آن بلوک

مرحله چهارم صحت سنجی داده های دریافتی:

در این مرحله داده های دریافت شده از نظر صحت اصالت داده و یکپارچگی مورد بررسی قرار می گیرد. برای این منظور تابع Verifier به صورت انتخابی یک عدد صحیح انتخاب کرده و برای شبکه ابری ارسال می کند.

$$chal = (c, k^{1}, k^{2})$$

$$1 \leq c \leq n, k^{1}, k^{2} \in Z*$$

شبکه ابری پس از دریافت این عدد تابع ji را ساخته و مقدار $R = gF^{\wedge}$ را به عنوان مرجع صحت اطلاعات محاسبه می کند.

$$ji = \pi k^{1}(i), ai = fk^{2}(i)$$

مشابه همین عملیات هم در زنجیره بلوک محاسبه شده و برای صحت سنجی به شبکه ابری ارسال می شود. پس از دریافت هر دو داده و مقایسه آن ها در صورت یکسان بودن مقدار تابع Verifier یعنی داده ها به صورت کامل دریافت شده و تغییری نکرده است.

# فصل ۳-  نقاط قوت و ضعف مقاله

مزایای این طرح :

۱- کارامد کردن روش های یکپارچگی داده بین کاربر و فضای ابری

۲- یک مدل ساخت یافته برای امنیت اطلاعات

۳- استفاده از روش های رمز نگاری قوی مثل rsa۲۵۶

۴- هزینه ارتباطی بهینه نسب به روش های مشابه

نقاط ضعفی که در این مقاله به آن اشاره نشده است:

۱- طرح پیشنهادی هم باید سمت کلاینت و هم فضای ابری پیاده سازی شود که در این صورت یکپارچگی شبکه تحت تاثیر قرار گرفته و کلیه عناصر متصل به شبکه باید از این روش استفاده کنند.

۲- هزینه محاسباتی بالا به خصوص در مواقعی که در آخرین مرحله صحت سنجی یکپارچگی داده ، خطا در صحت اطلاعات تشخیص داده شود ، ارسال و کلیه محاسبات باید مجدد از اول بررسی شود که این مورد باعث سربار هزینه با استفاده از این روش پیشنهادی است.

۳- در این روش از عبارت احتمال ناچیز [۱] برای مواقعی که محاسبات پارامترهای یکپارچگی خودشان دچار اشکال شدند و صحت سنجی با همین شرایط انجام شده ، نام می برد که می بایست در تمام حالات و احتمال خرابی کل داده بررسی شود.

[۱] negligible probability

# فصل ۴-  جمع بندی

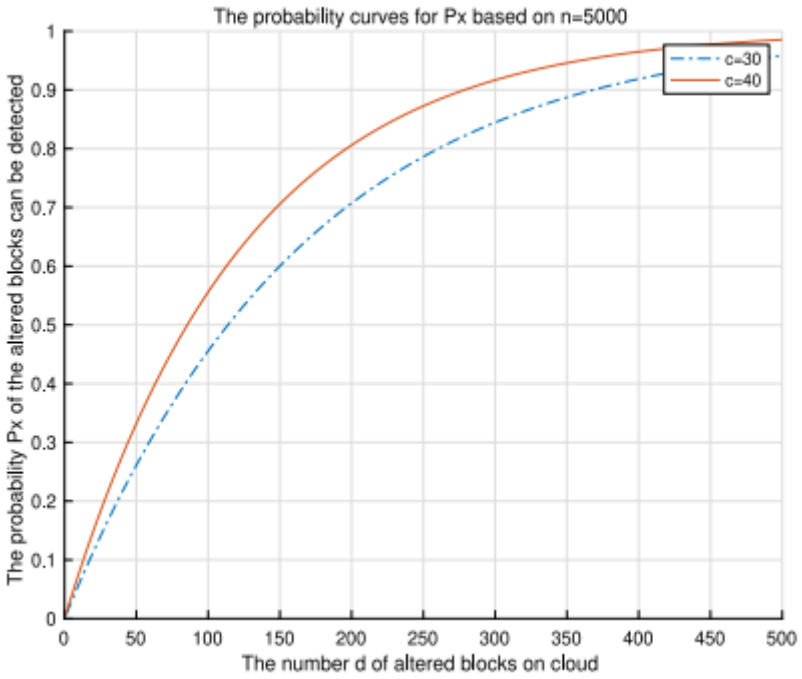
در G۵ ، وقتی داده های بسیار زیادی که از اینترنت اشیا در فضای ابر بارگذاری می شود، باید یکپارچگی داده ها از راه دور با یک مکانیزم کارآمد مورد بررسی قرار گیرد.
بر اساس خاصیت احراز هویت و صحت سنجی ای که زنجیره بلوک ها دارند ، این روش بر اساس زنجیره بلوک ها برای بررسی یکپارچگی داده از راه دور مورد استفاده قرار گرفته است. به این صورت که با زنجیره بلوک ها و استفاده از الگوریتم RSA ، به یک الگوی راستی آزمایی کارآمد رسیده است.

## ۴-۱-  کارهای آینده

در دنیای واقعی ، داده ها را می توان به انواع مختلفی تقسیم بندی کرد.بر اساس نیاز به حریم خصوصی ، نیازهای امنیتی ، مالکیت داده ها و غیره. انواع مختلف داده به طرح های مختلف بررسی یکپارچگی نیاز دارند. همچنین هنگامی که داده ها به نهادها مختلف تعلق دارد ، لازم است RDIC چند مالکیتی با استفاده از روش محاسبات امن چند طرفه مورد بررسی قرار گیرد.
برای داده های گزارش ، حریم خصوصی و قابلیت ردیابی داده مهم است. همچنین الزامات امنیتی حفظ اطلاعات گزارشگر مهم است. با توجه به اینکه بررسی صحت داده ها از راه دور با در نظر گرفتن حریم خصوصی یک چالش در طرح های مشابه می باشد، ارائه یک راهکار امن از اهمیت بسزایی برخوردار است.

## ۴-۲- نتایج شبیه سازی

جهت تحلیل هزینه محاسبات و ارتباطات با این روش از روش های ریاضی استفاده شده است. در نمودار شکل ۳ منحنی احتمال کشف خرابی در داده های دریافتی با استفاده از روش پیشنهادی را نشان می دهد. در این نمودار محور x تعداد بلوک های شبکه را نشان داده و محور y احتمال اینکه در این تعداد بلوک بتوان داده خراب را تشخیص داد ، نشان داده شده است. به عنوان مثال وقتی تابع challenge با مقدار ۳۰ مقدار دهی شده باشد، در تعداد ۴۵۰ بلوک احتمال تشخیص خرابی ۹۴,۱۵ ٪ می باشد.




**شکل ۳منحنی احتمال PX برای کشف خرابی داده**

در شکل ۴ مدت زمان پردازش یک داده ۱ ترابایتی با این روش در هر سمت نشان داده شده است.

**Table 2**
Computation cost of the parties (F = 1T bit, c = 50).

| Size of *l* | *Cloud* | *Blockchain* | *Client* | *Verifier* |
|---|---|---|---|---|
| 32 768($2^{15}$) | 0.6702 s | 0.0835 s | 137.5732 s | 0.6201 s |
| 65 536($2^{17}$) | 2.3254 s | 0.3145 s | 113.3259 s | 2.1372 s |
| 524 288($2^{19}$) | 8.1773 s | 1.023 s | 100.7351 s | 6.7715 s |

**شکل ۴ محاسبه هزینه پردازش داده ها با این روش**

# فصل ۵- منابع


[۱] G. ,. G. Miers, “Anonymous distributed e-cash from bitcoin ”,*IEEE* .۲۰۱۳ ,

[۲] S. Ron, “analysis of the full bitcoin transaction graph ”,*FC* .۲۰۱۳ ,

[۳] Z. ,. ,. Gao, “ A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks ”,*IEEE network* .۲۰۲۱ ,

[۴] H. ,. ,. G. Wang, “Blockchain-based anonymous reporting Blockchain-based anonymous reporting ”,*IEEE Trans* .۲۰۲۱ ,

[۵] X. Y. Tong, “Xiaohong sharding protocol for multi-domain iot blockchains ”, *Proceedings of IEEE International Conference on Communications* .۲۰۱۹ ,

[۶] Z. ,. Zhuang, “Blockchain for cyber security in smart grid A comprehensive survey ”, *IEEE Trans* .۲۰۲۱ ,

[۷] H. Wang, “Blockchain-based private provable data possession ”,*IEEE Trans* .۲۰۲۱ ,

[۸] S. ,. W. Gomez, “Machine learning aided scheme for load balancing in dense IoT networks ”,*Sensors* .۲۰۱۸ ,

[۹] S. ,. Talaat, “A load balancing and optimization strategy (LBOS) using reinforcement learning in fog computing environment ”,*Humaniz. Comput* .۲۰۲۰ ,

[۱۰] T. ,. Enokido, “The redundant energy consumption laxity based algorithm to perform computation processes for IoT services ”,*Internet Things* .۲۰۲۰ ,

[۱۱] D. ,. Kumar Kashyap, “Green computing in sensors-enabled internet of things: Neuro fuzzy logic-based load balancing ”,*Electronics* .۲۰۱۹ ,

[۱۲] A. ,. Adhikari, “ Heuristic-based load-balancing algorithm for IaaS cloud ”,*Future Gener. Comput* .۲۰۱۸ ,

[۱۳] B. ,. M. Swarna, “Load balancing of energy cloud using wind driven and firefly algorithms in internet of everything ”,*Parallel Distrib Comput* .۲۰۲۰ ,

[۱۴] K. ,. Rajaram, “Multi-hop optimized routing algorithm and load balanced fuzzy clustering in wireless sensor networks ”,*Humaniz Comput* .۲۰۲۰ ,

[۱۵] H. ,. Cui, “A load balancing routing mechanism based on SDWSN in smart city ”, *Electronics* .۲۰۱۹ ,

[١٦] G. ,. ,. L. Rego, “Software defined network-based control system for an efficient traffic management for emergency situations in smart cities ”,*Future Gener. Comput ,* ٢٠١٨.