Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

A Review of CP-ABE Access Control Schemes In Fog Computing

Mohammad Ali Alizadeh[1], Somayyeh Jafarali Jassbi[2*], Ahmad Khademzadeh[3]
[1]PhD student, Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
mohammadali.alizadeh@srbiau.ac.ir
[2]Assistant Professor, Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran
s.jassbi@srbiau.ac.ir
[3]Professor, ICT Research Institute, Tehran, Iran
zadeh@itrc.ac.ir

Abstract: Fog computing with cloud computing is useful for real-time processing in the IoT ecosystem. Fog computing can be used to outsource and lighten the computations of the end nodes because it is closer to the end nodes and has higher processing and communication power. On the other hand, the privacy and security of users of IOT are significant.This can be achieved by attribute encryption fine-grained access control schemes like ciphertext-policy attribute-based encryption (CP-ABE). Along with the improvements of the mentioned schemes, there are challenges such as attribute revocation and user revocation. In this article, we intend to review the new schemes based on CP-ABE, examine their extensive capabilities, and find an approach to the challenges each of them tried to solve. Also, clarify the architectural details of the mentioned designs implemented in the fog computing framework, such as the access policy model, attribute authority model, and underlying operations. Finally, we examine the weak points of the schemes to predict future development trends and present open issues.

Keywords: IoT, Fog computing, Access control, CP-ABE, RNS

JCDSA, Vol. 2, No. 3, Autumn 2024	Online ISSN: 2981-1295	Journal Homepage: https://sanad.iau.ir/en/Journal/jcdsa
Received: 2024-08-12	Accepted: 2024-11-26	Published: 2024-12-20

CITATION

Alizadeh, M.A., et al., " *A review of CP-ABE access control schemes in fog computing",* Journal of Circuits, Data and Systems Analysis (JCDSA), Vol. 2, No. 3, pp. 16-30, 2024.
DOI: 00.00000/0000

* Corresponding author

Extended Abstract

1- Introduction

To maintain the confidentiality and privacy of users in the Internet of Things (IoT) network, it is necessary to benefit from access control schemes. One of the most practical access control schemes in the IoT ecosystem is based on attribute-based encryption (ABE). The most important feature of these designs is granularity and support for one-to-many public key encryption algorithms. These features help secure and efficient authentication and authorization of multiple users with minimal need for key management. Designs based on ABE are divided into two general models: CP-ABE and KP-ABE. In general, the framework of these schemes includes four algorithms: setup, key generation, encryption, and decryption. In the less-used KP-ABE model, each data user must decrypt the ciphertext based on an access structure they define and a secret key provided by the data owner. The access structure and secret key are determined based on the attributes of the data users. This scheme has received less attention due to the inflexibility of the data owner in defining the access policy. However, the CP-ABE design, which is designed in contrast to KP-ABE, has been highly regarded due to its flexible and fine-grained structure. The data owner defines and encrypts the plaintext based on an access structure. If the data user's secret key can satisfy the access structure, it can decrypt the ciphertext. The main drawback of these two models is the underlying operation of bilinear pairing, which has a high computational overhead. Also, the operation of revoking users and their attributes is not agile. For this purpose, in many types of research, the authors outsourced operations with high overhead to the cloud server to lighten the calculations. However, the cloud server is not a suitable option due to its centralized structure and long distance from the end nodes, which often have limited processing resources. Therefore, in relatively recent research, designers took advantage of fog computing architecture with cloud computing. The RNS-ABE model was introduced as a special case in which the ABE access control scheme uses the residue number system (RNS) instead of bilinear pairing.

2- Methodology

This article first introduces basic concepts and definitions in the field of ABE, such as bilinear pairing, basic CP-ABE access control scheme, RNS, RNS-based access structures, access tree and LSSS, IoT for health and transportation, and proxy re-encryption (PRE) are discussed. Then, we reviewed and analyzed the latest articles in the field of ABE that implemented the infrastructure of fog computing and cloud computing in their architecture. In the end, the most relevant and newest articles have all implemented fog calculations from the perspective of the access structure model, attribute authority model, attribute and user revocation capabilities, underlying operations and other plugin capabilities such as hiding the access structure or blockchain implementation has been compared to be a basis for researchers in the field of ABE.

3- Results and discussion

In recent articles, more attention has been paid to the implementation of blockchain and it has been used in entities such as multiple attribute authority and fog computing. In addition, due to the high computational overhead of bilinear pairing, the focus has been on the underlying operations such as RNS, so that the calculations are inherently fast and there is no need to outsource expensive operations to fog calculations. Another shortcoming of CP-ABE schemes is the obviousness of the access structure embedded in the ciphertext, which some researchers have introduced ideas to hide from data users. Another challenge of these plans, which Bettencourt, the creator of the CP-ABE basic plan, also acknowledges, is the revocation of attributes and users, which have not been considered in many plans. In some designs, only one of the two has been given attention. Of course, all these designs have used PRE, which imposes a high computational overhead. In one of the research studies, the concept of user cooperation for decrypting the ciphertext was discussed, which is a practical and interesting idea.

4- Conclusion

ABE schemes are one of the most practical access control schemes that maintain user confidentiality, privacy, and security of devices and sensors in the IoT. The most important and flexible model of these designs is CP-ABE. This model has features such as granularity, the ability to design an access policy by the data owner, and easier management of encryption keys due to their one-to-many nature. But along with its advantages, it also has challenges and drawbacks. Their underlying operations, such as bilinear pairing and powering, have a high computational overhead, and features such as revocation of attributes, revocation of users, key escrow, non-confidentiality of the access policy embedded in the ciphertext, and the use of a single attribute authority, which will reduce its scalability; It has a challenge. Several solutions have been used to solve the above issues, such as fog computing implementation, multiple attribute authorities, blockchain, and using operations such as RNS and XOR instead of bilinear pairing. In the future, we suggest designing revocation algorithms in RNS, combining blockchain and RNS, and creating additional features such as hiding and user cooperation in RNS.

Islamic Azad University , Shiraz Branch
نشریه تحلیل مدارها، داده ها و سامانه ها
Journal of Circuits, Data and Systems Analysis
sanad.iau.ir/journal/jcdsa

مروری بر طرح‌های کنترل دسترسی رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز در محاسبات مه

محمدعلی علی‌زاده[۱]، سمیه جعفرعلی جاسبی*[۲]، احمد خادم‌زاده[۳]

۱- دانشجوی دکتری، گروه مهندسی کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (mohammadali.alizadeh@srbiau.ac.ir)

۲- استادیار، گروه مهندسی کامپیوتر، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (s.jassbi@srbiau.ac.ir)

۳- استاد، پژوهشگاه ارتباطات و فناوری اطلاعات، تهران، ایران (zadeh@itrc.ac.ir)

چکیده: محاسبات مه در کنار رایانش ابری توسعه مناسبی را برای پردازش‌های بلادرنگ در اینترنت اشیاء فراهم می‌کند. محاسبات مه به دلیل نزدیکی به گره‌های پایانی و دارابودن قدرت پردازشی و ارتباطی بالاتر، می‌تواند برای برون‌سپاری و سبک‌وزن سازی محاسبات گره‌های پایانی مورد استفاده قرار گیرد. از سوی دیگر حفظ حریم خصوصی و امنیت کاربران در اینترنت اشیاء نیز دارای اهمیت است. این مهم توسط طرح‌های کنترل دسترسی رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز (CP-ABE) به‌صورت ریزدانه و منعطف قابل‌دستیابی است. در کنار محسنات طرح‌های مذکور، چالش‌هایی نیز نظیر ابطال ویژگی و ابطال کاربر وجود دارد. در این مقاله در نظر داریم ضمن مرور طرح‌های نوین مبتنی بر CP-ABE به بررسی قابلیت‌های افزونه آنها نیز بپردازیم و به رهیافتی از چالش‌هایی که هر یک تلاش نمودند تا حل نمایند پی ببریم. همچنین جزئیات معماری هریک از طرح‌های مذکور را که در چارچوب محاسبات مه پیاده‌سازی شده‌اند نظیر مدل خط‌مشی دسترسی، مدل مرجع ویژگی و عملیات زیربنایی روشن نماییم. در پایان به بررسی نقاط ضعف طرح‌ها می‌پردازیم و روندهای توسعه آینده را پیش‌بینی می‌کنیم و مسائل باز را ارائه می‌دهیم.

واژه‌های کلیدی: اینترنت اشیاء، محاسبات مه، کنترل دسترسی، رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز (CP-ABE)، سیستم اعداد مانده‌ای (RNS)

نوع مقاله: مروری

تاریخ ارسال مقاله: ۱۴۰۳/۰۵/۲۲ تاریخ پذیرش مقاله: ۱۴۰۳/۰۹/۰۶ تاریخ چاپ مقاله: ۱۴۰۳/۰۹/۳۰

DOI: 00.00000/0000

۱- مقدمه

با محبوبیت ارتباطات نسل پنجم[۲]، تحقیقات در مورد کاربرد اینترنت اشیاء[۳] به طور فزاینده‌ای افزایش‌یافته است. برنامه‌های کاربردی اینترنت اشیاء بیشتر و بیشتر در زندگی روزمره مردم ظاهر می‌شوند. اینترنت اشیاء به اشیاء فیزیکی، اجازه تولید و تبادل داده می‌دهد، بنابراین خدمات هوشمند مختلفی را به کاربران ارائه می‌دهد. استفاده از اینترنت اشیاء تنها به ارائه خدماتی مانند دفاتر هوشمند، خانه‌های هوشمند و غیره محدود نمی‌شود، بلکه در حوزه صنایع مختلف نیز مانند شبکه‌های انرژی، مراقبت‌های بهداشتی، سیستم‌های حمل‌ونقل نیز گسترش‌یافته است. امروزه، اکثر کسب‌وکارهای جدید به روشی از طریق فناوری اینترنت اشیاء پشتیبانی می‌شوند. مشاهده می‌شود که ساعت دیجیتال به یک ساعت هوشمند، تلفن همراه به یک تلفن هوشمند، و عینک‌آفتابی به یک عینک هوشمند در حال تکامل است. به‌عبارت‌دیگر اینترنت اشیاء مجموعه‌ای از حسگرها، نرم‌افزارها و محرک‌های تعبیه‌شده در دستگاه‌هایی است که از طریق اینترنت برای ایجاد هوش با یکدیگر در ارتباط هستند و از طریق جمع‌آوری، پردازش و مبادله داده‌های تولید شده، خدمات موردنیاز را ارائه می‌دهند [۱].

اگرچه اینترنت اشیاء راحتی را در زندگی ما به ارمغان می‌آورد، اما تجزیه‌وتحلیل، محاسبه و ذخیره حجم عظیم‌داده‌های تولید شده برای دستگاه‌های اینترنت اشیاء چالش‌برانگیز است؛ زیرا چنین دستگاه‌هایی به‌طورکلی منابع محدودی باتوجه‌به توانایی‌های ذخیره‌سازی و پردازش دارند. برای غلبه بر این، رایانش ابری به‌عنوان یک راه‌حل بالقوه ظاهر شده است. رایانش ابری فناوری اطلاعات را متحول کرده است و در آن، نرم‌افزارها و زیرساخت‌های فناوری اطلاعات به‌عنوان یک سرویس در دسترس هستند. هزینه‌های سرمایه‌گذاری اولیه را کاهش می‌دهد، زمان راه‌اندازی زیرساخت را کوتاه می‌کند و خدمات مبتنی بر درخواست را به کاربران نهایی ارائه می‌کند. بااین‌حال، برای برنامه‌های حساس به تأخیر

* نویسنده مسئول

[2] 5G
[3] Internet of Things (IoT)

و موقعیت جغرافیایی مانند ایمنی در برابر آتش، نظارت بر سلامت و خودروهای خودران، نامناسب است. علاوه بر این، حجم داده‌های تولید شده توسط دستگاه‌های اینترنت اشیاء می‌تواند باتوجه‌به نیازهای برنامه، زیاد و مکرر باشد؛ بنابراین، ارسال تمام داده‌ها به ابر برای تجزیه‌وتحلیل، پردازش و ذخیره‌سازی به طور قابل‌توجهی بر پهنای باند شبکه تأثیر نامطلوب می‌گذارد. علاوه بر این، منابع ابری فقط از طریق اینترنت قابل‌دسترسی هستند و وجود یک اتصال پایدار به اینترنت پرسرعت، ممکن است برای دستگاه‌های اینترنت اشیاء امکان‌پذیر نباشد [۲].

برای مقابله با چالش‌های مذکور، الگوی محاسبات مه معرفی گردید. اساساً، محاسبات مه نوعی زیرساخت غیرمتمرکز است که در آن منابع محاسباتی و ذخیره‌سازی در اختیار دستگاه‌های اینترنت اشیاء به‌صورت بلادرنگ قرار گرفته و کمک به پردازش، تجزیه‌وتحلیل، ذخیره‌سازی داده‌ها و تسهیل ارتباط با ابر می‌کند. به‌عبارت‌دیگر، محاسبات مه گسترش رایانش ابری در لبه شبکه است و کمک می‌کند تا دستگاه‌های اینترنت اشیاء به ابر متصل و کیفیت خدمات بهبود بخشیده شود. بااین‌حال، برون‌سپاری داده‌های حساس برای پردازش و ذخیره‌سازی به گره‌های ثالث (ابر و مه) خطر امنیت داده‌ها و نقض حریم خصوصی را افزایش می‌دهد؛ زیرا این گره‌ها ممکن است دسترسی غیرمجاز داشته باشند یا ممکن است داده‌ها را برای منافع مالی به اشتراک بگذارند؛ بنابراین، تأمین امنیت داده‌های برون‌سپاری شده یک جنبه جدایی‌ناپذیر از محاسبات مه و رایانش ابری است. برای تأمین امنیت داده‌های برون‌سپاری شده، رمزگذاری قبل از برون‌سپاری رویکرد مناسبی است. بااین‌حال، سیستم‌های رمزنگاری سنتی مانند رمزنگاری با کلید متقارن یا رمزنگاری با کلید عمومی نمی‌توانند برای چنین اهدافی مورداستفاده قرار گیرند، زیرا نمی‌توانند کنترل دسترسی دقیق و ریزدانه، مدیریت و توزیع کلید کارآمد را فراهم کنند [۲].

در محیط‌های گسترده، به‌ویژه محیط‌های ابری، فناوری‌های رمزگذاری متقارن با کلید یکسان برای رمزگذاری و رمزگشایی از مشکلات توزیع و مدیریت کلید رنج می‌برند. بااین‌حال، روش‌های رمزگذاری نامتقارن مانند زیرساخت کلید عمومی[1] که از کلیدهای عمومی و خصوصی استفاده می‌کنند، فاقد کارایی محاسباتی هستند، زیرا مالکان داده‌ها باید هویت هر گیرنده و کلید عمومی آنها را از قبل مشخص کنند تا الگوریتم رمزگذاری را پیاده‌سازی کنند و متن رمزگذاری شده مختص هر گیرنده را به طور جداگانه ارسال کنند. در واقع زیرساخت کلید عمومی، مجموعه‌ای از ابزارها، رویه‌ها، سیاست‌ها، نرم‌افزارها و سخت‌افزارهایی است که برای ایجاد، مدیریت، توزیع، استفاده، ذخیره‌سازی و ابطال گواهینامه‌های دیجیتالی و کلیدهای عمومی استفاده می‌شود [۳]. هرچند هدف زیرساخت کلید عمومی، آسان‌تر کردن و امن‌تر کردن انتقال اطلاعات از طریق اینترنت است اما فرایند رمزگذاری باتوجه‌به تعداد گیرندگان کلید تکرار می‌شود و منجر به ایجاد سربار محاسباتی و ارتباطی می‌شود. ازآنجایی‌که نمی‌توان از این نوع زیرساخت برای یک‌بار رمزگذاری داده‌ها و ارسال آن به چندین کاربر استفاده کرد، رمزنگاری ویژگی مبنا[2] به‌عنوان راه‌حل مناسبی برای کاهش سربار محاسباتی بالای عملیات رمزگذاری سنتی و حفظ محرمانگی داده‌ها، اشتراک‌گذاری داده‌ها و کنترل دسترسی ریزدانه و منعطف توسط ساهای و واترز[3] ارائه شد [۴].

این یک مکانیسم رمزگذاری است که به کاربران اجازه می‌دهد تا داده‌ها را باتوجه‌به ویژگی‌های خود، مانند سن، جنسیت، تخصص، محل اشتغال، پست سازمانی و غیره، رمزگذاری و رمزگشایی کنند. رمزنگاری ویژگی مبنا، یک تکنیک رمزنگاری نامتقارن برای رمزگذاری یک به چند است که درک سنتی از رمزگذاری کلید عمومی را تغییر داد. در رمزگذاری سنتی با کلید عمومی، پیام برای یک گیرنده خاص با استفاده از کلید عمومی گیرنده رمزگذاری می‌شود. در مقابل، در رمزنگاری ویژگی مبنا، یک کلید عمومی برای کنترل دسترسی به داده‌های رمزگذاری شده، با استفاده از سیاست‌ها و ویژگی‌های دسترسی استفاده می‌شود [۵]. کاربردی‌ترین مدل رمزنگاری ویژگی مبنا، مدل مبتنی بر خط‌مشی متن رمز[4] است که توسط بتنکورت[5] و همکاران [۶] معرفی گردید. عملیات زیربنایی در این طرح، زوج نگار دوخطی[6] است.

۲- مبانی نظری

در ادامه مفاهیم و عملیات پایه‌ای در حوزه CP-ABE بیان می‌شود.

۲-۱- تعاریف

زوج نگار دوخطی:

اگر G_1 و G_T دو گروه چرخه‌ای ضربی از مرتبه اول p[7] باشند و سه شرط زیر صادق باشد، آنگاه $e: G_1 \times G_1 \rightarrow G_T$ یک نقشه زوج نگار دوخطی است [۷].

- دوخطی بودن[8]: برای هر $g_1, g_2 \in G_1$ و $a, b \in Z_p$ داریم:

$$e(g_1^a, g_2^b) = e(g_1^b, g_2^a) = e(g_1, g_2)^{ab} \quad (۱)$$

- عدم انحطاط[9]: برای هر $g_1, g_2 \in G_1$ معادله $e(g_1, g_2) = 1$ وجود ندارد.
- قابلیت محاسبه[10]: برای هر $g_1, g_2 \in G_1$، می‌توانیم $e(g_1, g_2)$ را به طور موثر محاسبه کنیم.

درخت دسترسی:

فرض می‌شود درخت دسترسی T باریشه r، یک ساختار (خط‌مشی) دسترسی را نشان می‌دهد [۶]. هر گره غیر برگ درخت نشان‌دهنده یک دروازه آستانه است که توسط فرزندان آن و یک مقدار آستانه توصیف

[1] Public Key Infrastructure (PKI)
[2] Attribute-based encryption (ABE)
[3] Sahai و Waters
[4] Ciphertext policy attribute-based encryption (CP-ABE)
[5] Bethencourt
[6] Bilinear pairing
[7] Multiplicative cyclic group of prime order p
[8] Bilinearity
[9] Non degeneracy
[10] Computability

شده است. اگر num_x تعداد فرزندان یک گره x و k_x مقدار آستانه آن باشد، $0<k_x\leq num_x$ است. (یعنی اگر هر k_x یا تعداد بیشتری از فرزندان گره x راضی باشند، گره x راضی است.) وقتی $k_x=1$ باشد، دروازه آستانه یک گیت OR و وقتی $k_x=num_x$ باشد، یک گیت AND است. هر گره برگ x با یک ویژگی و یک مقدار آستانه $k_x=1$ توصیف می‌شود. برای تسهیل کار با درخت‌های دسترسی، چند تابع تعریف می‌شود. والد گره x در درخت را با $parent(x)$ نشان می‌دهیم. تابع $att(x)$ تنها در صورتی تعریف می‌شود که x یک گره برگ باشد و نشان‌دهنده ویژگی مرتبط با گره برگ x در درخت باشد. درخت دسترسی T نیز ترتیبی را بین فرزندان هر گره تعریف می‌کند، یعنی فرزندان یک گره از ۱ تا num شماره‌گذاری می‌شوند. تابع $index(x)$ چنین عددی را مرتبط با گره x برمی‌گرداند. زیر درخت T که ریشه آن گره x است با T_x نشان داده می‌شود. اگر مجموعه‌ای از ویژگی‌ها که γ نامیده می‌شود، درخت دسترسی T_x را راضی کند، آن را به‌صورت $T_x(\gamma)=1$ نشان می‌دهیم. $T_x(\gamma)$ را به‌صورت بازگشتی بدین صورت محاسبه می‌کنیم که اگر x یک گره غیر برگ باشد، $T_{x'}(\gamma)$ را برای همه فرزندان x' از گره x محاسبه می‌کنیم. $T_x(\gamma)$ مقدار ۱ را برمی‌گرداند اگر و فقط اگر حداقل k_x فرزندان، ۱ را برگردانند. اگر x یک گره برگ باشد، آنگاه $T_x(\gamma)$ مقدار ۱ را برمی‌گرداند اگر و فقط اگر $att(x)\in\gamma$.

طرح به‌اشتراک‌گذاری راز خطی[1]:

این طرح [۷] اغلب برای تعریف خط‌مشی دسترسی در طرح‌های مبتنی بر خط‌مشی متن رمز استفاده می‌شود. با اعمال طرح اشتراک‌گذاری راز خطی، انتظار داریم فقط مجموعه‌های ویژگی مجاز که خط‌مشی دسترسی را برآورده می‌کنند، بتوانند به عدد مخفی $s\in Z_p$ دسترسی داشته باشند. خط‌مشی دسترسی مبتنی بر اشتراک‌گذاری راز خطی دارای دو جزء است: ماتریس تولید سهم[2] و تابع نگاشت $\rho()$ از دو الگوریتم تشکیل شده است: $share(s,(A_{l\times n},\rho()))$ و $reconstruction(S,\{\lambda_x\}_{x\,\epsilon\,l},\ (A_{l\times n},\rho()))$. ابتدا، مالک داده که مسئول تعریف خط‌مشی دسترسی است $A_{l\times n}$ را تشکیل می‌دهد. ماتریس تولید سهم دارای l ردیف و n ستون است. همه عناصر $A_{l\times n}$ باید در محدوده Z_p باشند. l همچنین برابر است با تعداد کل ویژگی‌های مورد استفاده در خط‌مشی دسترسی. n برابر است با پیچیدگی الگوریتم‌های $share()$ و $reconstruction()$. سپس تابع $\rho()$ را تشکیل می‌دهد. این تابع هر ردیف از $A_{l\times n}$ را دریافت می‌کند، به عنوان مثال، ردیف x یا A_x، در ورودی، و یک ویژگی متناظر $attr_x$ در خط‌مشی دسترسی در خروجی تولید می‌کند.

- $share\left(s,(A_{l\times n},\rho(x))\right)$:

ابتدا، مالک داده یک ماتریس عمودی $\vec{v}=(s,v_2,v_3,\cdots,v_n)^T$ را تشکیل می‌دهد. اولین عضو آن s است. $n\text{-}1$ عضو دیگر از اعداد تصادفی در محدوده Z_p تشکیل شده‌اند. سپس، سهام $\{\lambda_x=A_x\times\vec{v}\}_{x\,\epsilon\,l}$ را محاسبه می‌کند. به عبارت دیگر، $\vec{\lambda}=(\lambda_1,\lambda_2,\lambda_3,\cdots,\lambda_l)$ یک ماتریس ردیفی است که اعضای آن در محدوده Z_p قرار دارد و برای هر ویژگی در خط مشی دسترسی یک عضو وجود دارد.

- $reconstruction(S,\{\lambda_x\}_{x\,\epsilon\,l},\ (A_{l\times n},\rho()))$

مجموعه ویژگی‌های کاربر S (حرف بزرگ) را که در کلید محرمانه خود تعبیه شده است به‌عنوان ورودی دریافت می‌کند. اگر مجموعه مجاز باشد، مجموعه ثابت‌ها $\{w_x\in Z_p\}_{x\,\epsilon\,I}$ برای $I=\{x:\rho(x)\in S\}\subseteq\{1,2,\cdots,l\}$ از طریق معادله $\sum_{x\,\epsilon\,I}w_x\times A_x=(1,0,0,\cdots,0)$ با پیچیدگی زمانی چندجمله‌ای محاسبه می‌شود. سپس از طریق معادله $\sum_{x\,\epsilon\,I}w_x\times\lambda_x$، s محاسبه شده و در خروجی قرار می‌گیرد.

۲-۲- رمزگذاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز

بتنکورت [۶] برای اولین‌بار طرح CP-ABE عملیاتی را مبتنی بر زوج نگار دوخطی و خط‌مشی درخت دسترسی معرفی نمود. در این طرح، ویژگی‌ها با کلید محرمانه کاربر مرتبط می‌شوند و متن رمزگذاری شده با خط‌مشی دسترسی مرتبط است؛ بنابراین، افراد مجاز، تنها در صورتی می‌توانند پیام را رمزگشایی کنند که کلیدهای مخفی آنها با ویژگی‌های مرتبط با خط‌مشی دسترسی متن رمز مطابقت داشته باشد. این اجازه می‌دهد تا داده‌های محرمانه رمزگذاری شده با استفاده از CP-ABE در سرورهای غیرقابل‌اعتماد مانند ابر، بدون اجرای کنترل‌های احراز هویت برای دسترسی به داده‌ها، ذخیره شود. باتوجه‌به ادبیات موجود، CP-ABE در مقایسه با تکنیک‌های رمزنگاری سنتی، مزایای بیشتری دارد. این مزایا به شرح زیر است [۵]:

- سطح بالایی از محرمانگی داده‌ها را فراهم می‌کند.
- مکانیزم کنترل دسترسی رمزگذاری شده را برای برنامه‌های کاربردی فراهم می‌کند.
- سربار ارتباطی را کاهش می‌دهد، زیرا تولید کلید محرمانه کاربر فقط یک‌بار اتفاق می‌افتد.
- در برابر تبانی مقاوم می‌شود، زیرا هر ویژگی با یک چندجمله‌ای یا یک عدد تصادفی مرتبط است که از تبانی کاربران قانونی با یکدیگر جلوگیری می‌کند.
- از مقیاس‌پذیری کاربران پشتیبانی می‌کند. با افزایش تعداد کاربران مجاز، سیستم می‌تواند به طور مؤثر کار کند.

این طرح از چهار الگوریتم پایه «راه‌اندازی، تولید کلید، رمزگذاری و رمزگشایی» به شرح زیر تشکیل شده است که در مقالات جدید مانند [۲،۹،۱۶] دچار تغییراتی گردید و قابلیت‌هایی نظیر ابطال و صحت‌سنجی عملیات برون‌سپاری شده به آن اضافه شد. هر کاربر داده دارای یک کلید محرمانه است که بر اساس ویژگی‌های متعلق به او ساخته می‌شود. هر مالک داده یک خط‌مشی (سیاست) دسترسی تعریف می‌کند تا تنها کاربران داده مجاز بتوانند آن را راضی نمایند و متعاقباً

[1] Linear Secret Sharing Scheme (LSSS)

[2] Share-generating matrix $A_{l\times n}$

بتوانند متن رمز را رمزگشایی کنند. خط‌مشی دسترسی در متن رمز جاسازی شده است و ساختارهای متنوعی دارند؛ مانند درخت دسترسی، اشتراک‌گذاری راز خطی و گیت‌های *AND* و *OR*.

۱. $Setup(1^k) \rightarrow PK, MK$: پارامتر امنیتی 1^k را به‌عنوان ورودی می‌گیرد و کلید عمومی PK و کلید مخفی اصلی MK را خارج می‌کند. g مولد گروه G_1 است.

$$PK = \left(G_1; g; h = g^{\beta}; f = g^{1/\beta}; e(g, g)^{\alpha}\right) \quad (۲)$$
$$MK = (\beta; g^{\alpha})$$

۲. $Keygen(PK, MK, S) \rightarrow SK$: مجموعه ویژگی‌های کاربر S، PK و MK را به‌عنوان ورودی می‌گیرد و کلید محرمانه SK کاربر را خارج می‌کند. $j \epsilon S$ و $r \epsilon Z_p$ و $r_j \epsilon Z_p$ است و همگی تصادفی هستند.

$$SK = \left(g^{(\alpha+r)/\beta}; \forall j \epsilon S : D_j = g^{r}.H(j)^{rj}; D'_j = g^{rj}\right) \quad (۳)$$

۳. $Enc(PK, PT, T) \rightarrow CT$: متن ساده PT، خط‌مشی دسترسی T و PK را به‌عنوان ورودی می‌گیرد و متن رمز CT را خارج می‌کند.

$H : \{0, 1\}^* \rightarrow G_1$ ،$q_r(0) = s$ و $q_{x(0)} = q_{parent(x)}(index(x))$ است. تابع H هر رشته دلخواه از ۰ و ۱ را به یک عضو یکتا گروه G_1 نگاشت می‌کند. Y مجموعه برگ‌های درخت دسترسی است. در طرح بتنکورت [۵]، خط‌مشی دسترسی از مدل درخت دسترسی است.

$$CT = \left(T; C' = PT.e(g; g)^{\alpha s}; C = h^{s}; \forall y \epsilon Y : C_y = g^{q_y(0)}.H(j)^{rj}; C'_y = g^{rj} = H(att(y))^{q_y(0)}\right) \quad (۴)$$

۴. $Dec(PK, SK, CT) \rightarrow PT$: SK و CT را به‌عنوان ورودی می‌گیرد. اگر S، T را برآورده کند، PT را خارج می‌کند. اگر گره x یک گره برگ باشد و $i = att(x)$، می‌بایست به‌صورت بازگشتی و به کمک تابع زیر عمل نمود تا پس از راضی شدن درخت دسترسی امکان رمزگشایی توسط کاربر داده مجاز فراهم شود. درصورتی‌که $i \neq att(x)$ باشد $DecryptNode(CT, SK, x) = \perp$ و عملیات ناتمام باقی می‌ماند. جزئیات بیشتر را می‌توانید در [۶] ملاحظه بفرمائید.

$$DecryptNode(CT, SK, x) = \frac{e(D_i, C_x)}{e(D_i, C_x)} = e(g, g)^{rq_x(0)} \quad (۵)$$

۲-۳- سیستم اعداد مانده‌ای

سیستم اعداد مانده‌ای[1] در [۸] به تفضیل این سیستم عددی نامتعارف معرفی شده است. در RNS ابتدا یک عدد صحیح بزرگ بر اساس تبدیل به جلو[2] به مجموعه‌ای از باقیمانده‌ها که اعداد صحیح کوچک هستند تبدیل می‌شود. سپس محاسباتی مانند جمع، تفریق و ضرب بر روی آنها انجام می‌شود. در پایان به کمک تبدیل معکوس[3] مجدداً مجموعه مانده‌ها به یک عدد صحیح بزرگ تبدیل می‌شود. در واقع حسن این سیستم، کمک به انجام محاسبات با سربار کمتر و به شکل موازی است. در تبدیل به جلو به ترتیب مراحل زیر را انجام می‌دهیم:

۱- مجموعه‌ای از اعداد صحیح نسبتاً کوچک را انتخاب می‌کنیم که نسبت به یکدیگر اول هستند و به آن مجموعه پیمانه $\{m_1, m_2, \cdots, m_n\}$ می‌گوییم.

۲- باقیمانده یک عدد صحیح دلخواه بزرگ X را نسبت به پیمانه‌های متعلق به مجموعه پیمانه با طول n را محاسبه می‌کنیم.

$$\{x_i \mid x_i = X \bmod m_i \ \ for\ 1 \leq i \leq n\} \quad (۶)$$

قضیه باقیمانده چینی[4] (CRT) و تبدیل ریشه مختلط[5] (MRC) دو تکنیک اصلی برای تبدیل معکوس هستند. اخیراً تکنیک‌های جدید مبتنی بر این دو روش مانند New CRT-I، New CRT-II و Mixed-Radix CRT نیز ارائه شده است [۸]. MRC ساختار سریال دارد و CRT ساختار موازی دارد. باتوجه‌به قابلیت‌های CRT، معمولاً از این روش استفاده می‌شود. جایی که $M_i = M/m_i$ برای $i = 1, 2, \ldots, n$ و $M = \prod_{i=1}^{n} M_i$ به عنوان محدوده دینامیکی شناخته می‌شود. هر عدد صحیح بزرگ تنها زمانی نمایش منحصر بفرد RNS دارد که مقدارش بین ۰ و محدوده دایناميکی باشد. $\left(\frac{1}{M_i}\right)_{m_i}$ به‌عنوان معکوس ضربی نسبت به پیمانه M_i شناخته می‌شود.

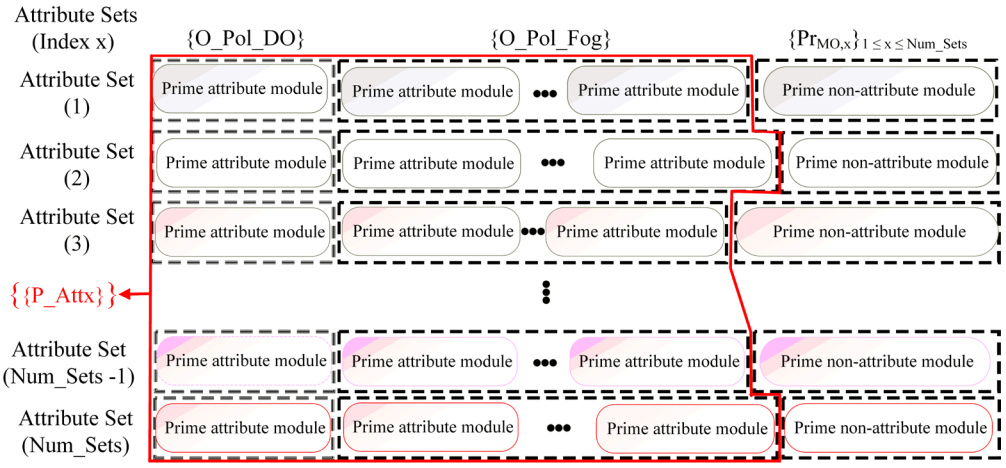
$$X = \sum_{i=1}^{n} x_i M_i \left(\frac{1}{M_i}\right)_{m_i} \bmod M \quad (۷)$$

$$\left(M_i \left(\frac{1}{M_i}\right)\right)_{m_i} = 1 \quad (۸)$$

۲-۴- خط‌مشی دسترسی سیستم اعداد مانده‌ای

مطابق با شکل (۱) هر ویژگی استفاده شده در این ساختار [۹] که دارای طول متغیر است، باید از طریق تابع هش SHA ۳-۵۱۲[6] به یک‌رشته عددی ۵۱۲ بیتی تبدیل شود. آن را ماژول ویژگی[7] نام‌گذاری می‌کنیم. در طول رمزگذاری، باقیمانده‌های یک عدد صحیح بزرگ را نسبت به ماژول‌های ویژگی محاسبه می‌کنیم. در واقع عدد صحیح بزرگ، متن ساده است و مجموعه باقیمانده‌ها نسبت به ماژول‌های ویژگی، متن رمز است. ازآنجاکه لازم است ماژول‌ها در سیستم اعداد مانده‌ای عدد اول[8] باشند، همه ماژول‌های ویژگی باید به یک عدد اول معادل تبدیل شوند؛ بنابراین، کوچک‌ترین عدد اول بزرگ‌تر از مقدار هر ماژول ویژگی را انتخاب می‌کنیم و آن را ماژول ویژگی اول[9] می‌نامیم.

[1] Residue number system (RNS)
[2] Forward conversion
[3] Reverse conversion
[4] Chinese Remainder Theorem
[5] Mixed Radix Conversion
[6] SHA3-512 hash function
[7] Attribute module
[8] Prime
[9] Prime attribute module



شکل (۱): خط‌مشی دسترسی سیستم اعداد مانده‌ای [۹]

در این طرح که هدف آن اجرای کنترل دسترسی ریزدانه با استفاده از رمزنگاری ویژگی مبنا است، ویژگی، ماژول ویژگی و ماژول ویژگی اول را برای سادگی معادل یکدیگر در نظر می‌گیریم. این ساختار یک آرایه دوبعدی است که در آن مجموعه معتبری از ماژول‌های ویژگی اول در هر سطر به جز آخرین ستون بارگذاری می‌شود. در هر ستون، یک ماژول ویژگی اول که عضوی از آن مجموعه است قابل‌بارگذاری است. تعداد سطرها برابر با Num_sets است و تعداد ستون‌های هر سطر می‌تواند متفاوت باشد. اگر ویژگی‌های متعلق به یک کاربر داده دقیقاً با ماژول‌های ویژگی اول هر خط از خط‌مشی دسترسی سیستم اعداد مانده‌ای مطابقت داشته باشد، می‌تواند آن را راضی نماید. هر خط از خط‌مشی دسترسی، یا به‌عبارت‌دیگر، هر مجموعه ویژگی که خط‌مشی دسترسی را تشکیل می‌دهد، از سه مدل ماژول به شرح زیر تشکیل شده است:

۱- مدل اول دارای طول ثابت ۵۱۲ بیت است و توسط مالک داده به ماژول‌های ویژگی اول تبدیل می‌شود. این ماژول‌ها همه، اعضای مجموعه $\{O\_Pol\_DO\}$ هستند. این مجموعه باید نزد مالک داده محرمانه بماند و به کاربر داده، مه و سرورهای ابری ارسال نخواهد شد. این امر امنیت را بهبود می‌بخشد و اگر دشمن به آنها نفوذ کند، از دسترسی به کل خط‌مشی دسترسی محروم می‌شود.

۲- مدل دوم دارای طول ثابت ۵۱۲ بیت است و توسط مالک داده تعریف شده است. بااین‌حال، برای تولید ماژول‌های ویژگی اول معادل، آنها به گره مه برون‌سپاری می‌شوند تا سربار محاسباتی را کاهش دهند. همه این ماژول‌ها اعضای مجموعه $\{O\_Pol\_Fog\}$ هستند. پس از تکمیل هر دو مجموعه $\{O\_Pol\_DO\}$ و $\{O\_Pol\_Fog\}$، مالک داده بخشی از خط‌مشی دسترسی را طراحی کرده و آنها را در ردیف‌های مرتبط قرار می‌دهد. ما آن را خط‌مشی دسترسی جزئی $\{\{P\_Attx\}\}$ می‌نامیم. سپس $\{\{P\_Attx\}\}$ را به مرجع ویژگی[1] ارسال می‌کند تا مدل سوم ماژول‌های موردنیاز را دریافت کند.

۳- مدل سوم نه یک ماژول ویژگی است و نه طول ثابت ۵۱۲ بیت دارد. طول این ماژول‌ها باید متناسب با طول متن ساده و طول هر ردیف از $\{\{P\_Attx\}\}$ باشد؛ بنابراین اعداد تصادفی با طول موردنظر تولید می‌شوند و متعاقباً مرجع ویژگی کوچک‌ترین عدد اول بزرگ‌تر از آنها را محاسبه می‌کند. ما آنها را ماژول‌های بدون ویژگی اول $\{Pr_{MO,x}\}$ می‌نامیم، جایی که MO کلید عمومی مالک داده است. برای مطالعه جزئیات بیشتر به مقاله [۹] مراجعه بفرمایید.

۲-۵- طرح‌های کنترل دسترسی مبتنی بر زنجیره قالب[2]

زنجیره قالب، یک دفترکل[3] غیرقابل‌تغییر است که شامل مجموعه‌ای از بلوک‌های مرتبط است که توسط استخراج‌کنندگان در یک شبکه همتا به همتا[4] تأیید شده‌اند [۱۰]. ویژگی‌های اصلی زنجیره قالب را می‌توان به‌صورت زیر خلاصه کرد:

- تمرکززدایی: جنبه غیرمتمرکز زنجیره قالب می‌تواند هر نقطه از شکست را از بین ببرد و در نتیجه تحمل خطا را بهبود بخشد. دستگاه‌های اینترنت اشیاء می‌توانند بدون دخالت هیچ واسطه‌ای با استفاده از زنجیره قالب با یکدیگر تعامل داشته باشند.
- توزیع: زنجیره قالب به‌عنوان یک دفترکل توزیع شده، توانایی ذخیره و توزیع داده‌ها را دارد. سیستم اعتبارسنجی بر روی گره‌های مختلف تضمین می‌شود.
- تغییرناپذیری: داده‌های موجود در زنجیره قالب را نمی‌توان تغییر داد. در واقع، زنجیره قالب دنباله‌ای از بلوک‌ها است که فهرست کاملی از تراکنش‌ها را در خود جای‌داده است. هر بلوک از طریق یک مرجع به بلوک قبلی اشاره می‌کند که اساساً یک مقدار هش بلوک قبلی است. هر گونه تغییر در یک بلوک منجر به قطع ارتباط بین بلوک‌ها می‌شود که تغییرناپذیری را تضمین می‌کند.

[1] Attribute Authority (AA)
[2] Block chain
[3] Ledger
[4] Peer-to-peer (P2P)

• مقیاس‌پذیری: فناوری زنجیره قالب می‌تواند جمع‌آوری و پردازش داده‌های صادر شده از تعداد زیادی از دستگاه‌های اینترنت اشیاء را کنترل کند.
• ناشناس بودن: امکان تعامل با یک آدرس کلی وجود دارد. اطلاعات شخصی برای افزودن تراکنش، ضروری نیست.

انواع زنجیره قالب را می‌توان به سه دسته زیر طبقه‌بندی کرد:

• عمومی: همه می‌توانند به شبکه بپیوندند و می‌توانند در فرایند اعتبارسنجی تراکنش‌ها (ماینینگ) شرکت کنند.
• خصوصی: برعکس زنجیره قالب عمومی است، زیرا یک شبکه محدود است که هر عضوی که می‌خواهد به شبکه بپیوندد باید توسط یک سازمان مجاز شناخته شود.
• مرکب: ترکیبی از زنجیره قالب خصوصی و عمومی است. فرایند اعتبارسنجی توسط شرکت‌کنندگان منتخب انجام می‌شود.

راه‌حل‌های کنترل دسترسی مبتنی بر زنجیره قالب را می‌توان به دو زیر طبقه تقسیم کرد: راه‌حل‌های ایستا که در آنها خط‌مشی کنترل دسترسی در ابتدا مشخص می‌شود و راه‌حل‌های پویا که در آنها خط‌مشی به دلیل شرایط مختلف می‌تواند به‌صورت پویا تغییر کند.

۲-۶- رمزگذاری مجدد پراکسی

رمزگذاری مجدد پراکسی[1] یک پروتکل رمزگذاری سراسری است که مقیاس‌پذیرتر و انعطاف‌پذیرتر از رمزگذاری کلید عمومی است و گروهی از موجودیت‌های پراکسی مانند رایانش ابری را قادر می‌سازد تا داده‌های رمزگذاری شده را از یک کلید عمومی به کلید عمومی دیگر تبدیل کنند، بدون اینکه قدرت رمزگشایی داده‌ها را یا دسترسی به هر کلید محرمانه را پیدا کنند [۱۱]. برای درک بهتر این پروتکل اجازه دهید با مثالی آن را توضیح دهیم. فرض کنید یک مالک داده بنام محمد و دو کاربر داده به نام علی و مجید در نظر گرفته‌ایم. یک گره میانی ابری نیز جهت اشتراک‌گذاری داده بین این سه شخص مستقر شده است. محمد در ابتدا می‌خواهد متن رمزی را با استفاده از رمزگذاری کلید عمومی تولید نماید، به شکلی که فقط علی بتواند رمزگشایی کند و برای گره ابر و مجید ناممکن باشد؛ بنابراین با کلید عمومی علی، متن رمز را تولید می‌کند و آن را در اختیار ابر قرار می‌دهد تا علی بتواند به آن دسترسی بیاید. پس از مدتی، نظرش عوض می‌شود و تصمیم می‌گیرد تا بجای علی، مجید بتواند متن رمز به اشتراک گذاشته شده در گره ابری را رمزگشایی کند. روش غیر امن و با سربار محاسباتی بالاتر، آن است که کلید محرمانه محمد برای گره ابری افشا شود تا متعاقباً پس از رمزگشایی آن توسط ابر و تولید متن ساده، با استفاده از کلید عمومی مجید مجدداً رمزگذاری شود. اما در روش رمزگذاری مجدد پراکسی، یک کلید محرمانه در اختیار پراکسی قرار داده می‌شود تا بدون افشا کلید محرمانه محمد و متن ساده، متن رمز را به شکلی تغییر یابد که دیگر تنها مجید آن را بتواند رمزگشایی نماید و امکان رمزگشایی توسط علی میسر نباشد. این روش در طرح‌های کنترل دسترسی مبتنی بر خط‌مشی متن رمز برای ابطال کاربر[2] یا ابطال ویژگی[3] کاربردی است. برای شناخت بهتر طرح‌هایی که از پروتکل رمزگذاری مجدد پراکسی استفاده نمودند، مطالعه [۱۱] پیشنهاد می‌شود.

۲-۷- اینترنت وسایل نقلیه مبتنی بر معماری محاسبات مه

اینترنت وسایل نقلیه[4] با توسعه اینترنت وسایل نقلیه [۱۲]، انواع برنامه‌های کاربردی وسایل نقلیه متنوع‌تر شده‌اند و در نتیجه، درخواست‌های خدمات ایجاد شده افزایش یافته‌اند. باتوجه‌به محدودیت قدرت محاسباتی و ذخیره‌سازی وسایل نقلیه، درخواست منابع برای بسیاری از وظایف محاسباتی دشوار است. علاوه بر این، مدل‌های خدمات محاسبات ابری سنتی از تراکم شبکه، تأخیر شبکه بالا و هزینه‌های عملیاتی بالا رنج می‌برند. برای این منظور، محاسبات مه خودرو[5] در حال ظهور است. در محاسبات مه خودرو، وسایل نقلیه با چندین حسگر نصب شده برای جمع‌آوری اطلاعات ترافیک عمل می‌کنند. از طریق فناوری ارتباطات بی‌سیم، وسایل نقلیه می‌توانند ارتباطات همه‌جانبه شبکه مانند خودرو به زیرساخت[6]، وسیله نقلیه به‌وسیله نقلیه[7] و غیره را تحقق بخشند. واحدهای کنار جاده[8] مستقر در جاده‌ها به‌عنوان گره‌های مه برای پاسخگویی به درخواست‌های خودرو در زمان واقعی عمل می‌کنند و خدمات متنوعی را برای وسایل نقلیه مانند جمع‌آوری داده‌ها، ناوبری و انتقال داده ارائه می‌دهند. به‌این‌ترتیب، محاسبات مه خودرو می‌تواند به طور قابل‌توجهی تأخیر شبکه را کاهش دهد و درعین‌حال به کاربران خدمات و تجارب رانندگی ایمن، آسان، هوشمند، و کارآمد ارائه دهد.

علی‌رغم مزایای بزرگی که محاسبات مه خودرو برای ما به ارمغان می‌آورد، دستیابی به‌اشتراک‌گذاری امن و مطمئن داده در آن یک چالش بزرگ است. داده‌های مبادله شده بین وسایل نقلیه، حاوی مقادیر زیادی اطلاعات خصوصی مانند مسیرهای رانندگی و هویت کاربران است. در این سیستم پیچیده، حریم خصوصی کاربر به‌راحتی می‌تواند به خطر بیفتد. علاوه بر این، کنترل دسترسی منعطف و ریزدانه در به‌اشتراک‌گذاری داده‌ها برای جلوگیری از دسترسی غیرمجاز بسیار مطلوب است. رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز یک رویکرد برجسته برای دستیابی به کنترل دسترسی دقیق و یک به چند است. مالکان داده‌ها[9]، مجاز به تدوین خط‌مشی‌های دسترسی هستند که با فراخوانی الگوریتم رمزگذاری در متن‌های رمز جاسازی می‌شوند. کلیدهای خصوصی توزیع‌شده کاربران داده[10] به ویژگی‌هایی که دارند مربوط می‌شود. کاربران داده، تنها در صورتی می‌توانند متن‌های رمزی

[1] Proxy re-encryption (PRE)
[2] User revocation
[3] Attribute revocation
[4] Internet of Vehicles
[5] Vehicular fog computing (VFC)
[6] Vehicle-to-infrastructure (V2I)
[7] Vehicle-to-vehicle (V2V)
[8] Road side units (RSU)
[9] Data Owner (DO)
[10] Data user (DU)

را رمزگشایی کنند و متن اصلی را کشف نمایند که ویژگی‌های آنها با خط‌مشی‌های دسترسی مطابقت داشته باشد.

بااین‌وجود، قبل از به‌کارگیری طرح کنترل دسترسی مبتنی بر خط‌مشی متن رمز در محاسبات مه خودرو، موارد عملی زیر باید در نظر گرفته شود [۱۲]:

۱. ابطال ویژگی ناکارآمد: در محاسبات مه خودرو، ویژگی‌های وسیله نقلیه ممکن است به طور مکرر برای الزامات برنامه‌های مختلف تغییر کند. هنگامی که کاربر، یک ویژگی را ابطال می‌کند، حق دسترسی مربوطه باید به‌سرعت ابطال شود. بااین‌حال، این موضوع پیچیده است. ازآنجایی‌که ویژگی‌های کاربر در سیستم معمولاً توسط همه کاربران استفاده می‌شود، هر ابطال ویژگی بر سایر کاربران ابطال نشده که آن ویژگی را نیز دارند، تأثیر می‌گذارد. یکی از راه‌های رایج برای مقابله با این مسئله، رمزگذاری مجدد متن رمزی مربوط به ویژگی ابطال‌شده برای کاربرانی است که ابطال نشده‌اند، اما همچنین باید اطمینان حاصل کنیم که این متون رمزگذاری شده مجدداً می‌توانند به طور معمول توسط کاربران موجود که در ابتدا دارای امتیاز دسترسی بودند، دسترسی داشته باشند. برای این منظور، طرح‌های موجود نیز از این کاربران می‌خواهند که کلیدهای رمزگشایی مربوطه خود را به‌روزرسانی کنند. عملیات پیچیده فوق هزینه‌های محاسباتی و ارتباطی زیادی را به همراه دارد. برای خودروهایی که به تأخیر کم و کارایی بالا نیاز دارند، انجام چنین عملیات پیچیده‌ای هر بار که یک ویژگی باطل می‌شود، به طور قابل‌توجهی غیرعملی است.

۲. ذخیره‌سازی متمرکز داده: طرح‌های اشتراک داده معمولاً داده‌های کاربر را در سرورهای ابری ذخیره می‌کنند. بااین‌حال، ازآنجایی‌که ابر یک شخص ثالث نیمه قابل‌اعتماد است، یک نقطه شکست وجود دارد. هنگامی که ابر توسط یک دشمن مورد حمله قرار می‌گیرد، ممکن است تمام داده‌های کاربر را فاش کند. به‌عنوان‌مثال، در سال ۲۰۱۷، مرکز امنیتی کرامتچ[1] دریافت که یک سرور متمرکز بیش از ۵۰۰۰۰۰ سوابق خودرو، از جمله وضعیت تجهیزات خودرو، مسیرهای رانندگی و غیره را به بیرون درز داده است و حریم خصوصی صدها هزار کاربر را به خطر انداخته است. خوشبختانه، ظهور فناوری زنجیره قالب ، اجرای ذخیره‌سازی داده‌های توزیع‌شده را امکان‌پذیر کرده است. بااین‌حال، زنجیره قالب نیاز به همگام‌سازی تمام داده‌ها از زمان تشکیل بلوک پیدایش[2] (بلوک پیدایش، اولین بلوکی است که ساخته می‌شود) دارد که منجر به کمبود جدی فضای ذخیره‌سازی در زنجیره قالب می‌شود.

۲-۸- اینترنت پزشکی اشیاء

اینترنت پزشکی اشیاء[3] با ظهور دستگاه‌های پزشکی قابل پوشیدن و کاشتنی و سایر فناوری‌هایی که امکان جمع‌آوری داده‌های پزشکی را فراهم می‌کند، اینترنت پزشکی اشیاء منجر به پیشرفت‌های فناوری در مراقبت‌های بهداشتی می‌شود [۵]. بااین‌حال این پیشرفت‌ها، چالش‌های زیادی را به‌ویژه برای امنیت و حریم خصوصی اطلاعات پزشکی ایجاد می‌کنند؛ بنابراین، حفظ محرمانگی و امن نمودن اطلاعات جمع‌آوری‌شده توسط دستگاه‌های اینترنت پزشکی اشیاء همچنان موضوع اصلی تحقیقاتی است. اگرچه ظهور محاسبات مه مشکلات متعددی را که در معماری‌های مبتنی بر رایانش ابر سنتی آشکار بود حل می‌کند، اما امنیت داده‌های پزشکی همچنان یک نگرانی است. معماری‌های فعلی که برای محافظت از داده‌ها توسعه یافته‌اند، توانایی‌های محدود دستگاه‌ها را در نظر نمی‌گیرند، مانند ظرفیت ذخیره‌سازی و انرژی که بر طول عمر دستگاه‌ها و اثربخشی آنها در گرفتن و ارسال سیگنال‌ها تأثیر می‌گذارد؛ بنابراین، به‌منظور اطمینان از حفاظت کافی از اطلاعات پزشکی، یک معماری امن مبتنی بر رایانش ابری و محاسبات مه موردنیاز است.

۳- مروری بر طرح‌های پیشین

بتنکورت و همکاران برای اولین‌بار یک مدل عملیاتی مبتنی بر خط‌مشی متن رمز بر اساس رمزنگاری مبتنی بر زوج نگار دوخطی ارائه نمود. مهم‌ترین مزیت این طرح رمزگذاری یک به چند است که به زیرساخت محاسبات ابری کاملاً مطمئن نیاز ندارد. بااین‌حال، مشکل اصلی این طراحی، عدم سادگی محاسبات ابطال کاربر و ابطال ویژگی است. همچنین، این طرح مستعد حملات تبانی است [۶]. در [۱۳]، یک طرح کنترل دسترسی کارآمد باقابلیت برون‌سپاری و به‌روزرسانی ویژگی با استفاده از محاسبات مه پیشنهاد شده است. در [۱۴] که اساس [۱۵] است، نویسندگان یک معماری چندلایه برای مرجع ویژگی بر اساس رمزنگاری ویژگی مبنا سلسله‌مراتبی[4] پیشنهاد کرده‌اند. علاوه بر این، با استفاده از امضای مبتنی بر ویژگی، تغییر مجاز داده‌ها تضمین می‌شود. بااین‌حال، محاسبات مه در این مقاله استفاده نشده است. سپس، نویسندگان در [۱۵] یک طرح برون‌سپاری داده امن و سبک‌وزن ارائه می‌کنند و بیشتر عملیات پرهزینه را از دستگاه‌های اینترنت اشیاء به گره‌های مه منتقل می‌کنند. همچنین امکان به‌روزرسانی متن رمز در زیرساخت ابری را با استفاده از امضای مبتنی بر ویژگی فراهم می‌کند. در [۱۶]، یک طرح یادگیری الکترونیکی امن و کارآمد مبتنی بر مه معرفی شده است و متعاقباً محاسبات مه را در سیستم آموزش الکترونیکی ادغام می‌کند تا تأخیر خدمات آموزش الکترونیکی ارائه شده را کاهش دهد. براین‌اساس، نویسندگان، یک طرح کم هزینه ترکیبی با کمک رمزنگاری ویژگی مبنا و رمزنگاری پخش مبتنی بر هویت[5] طراحی

[1] Kromtech
[2] Genesis Block
[3] Medical Internet of Things (MIoT)
[4] Hierarchical attribute-based encryption (HABE)
[5] Identity-Based Broadcast Encryption (IBBE)

می‌کنند. رمزنگاری پخش مبتنی بر هویت، یک روش کارآمد برای پخش یک پیام به چندین هویت پیشنهاد می‌دهد. در این روش متن رمز با یک لیست پخش هویت، رمزگذاری می‌شود به طوری که تنها کاربرانی که هویتشان به لیست تعلق دارد می‌توانند متن رمز را رمزگشایی کنند. برخلاف روش رمزنگاری پخش مبتنی بر هویت، رمزنگاری مبتنی بر هویت[1] سنتی باید پیام را به چندین گیرنده یک به یک و به ترتیب و نه همزمان ارسال کند. این قابلیت، بکارگیری روش رمزنگاری پخش مبتنی بر هویت را در بسیاری از برنامه های کاربردی مانند سیستم‌های ایمیل کارا می‌کند. با این حال، مشکل سپردن (ذخیره‌سازی) کلید[2]، یک چالش جدی است [۱۷].

نویسندگان [۱۸] ابتدا یک مدل رمزنگاری ویژگی مبنا به نام MABE[3] را با یک تابع هش مقاوم در برابر برخورد معرفی می‌کند. سپس از آن برای ایجاد یک سیستم کنترل دسترسی اشتراک‌گذاری داده در رایانش ابری استفاده می‌کند. طرح‌های مبتنی بر خط‌مشی متن رمز به‌ندرت بر ابطال کاربر و ابطال ویژگی در محاسبات مه تمرکز می‌کند و همچنان سربار محاسباتی و ذخیره‌سازی بالایی را بر روی دستگاه‌های اینترنت اشیاء با منابع محدود تحمیل می‌کند؛ بنابراین، [۱۹] یک طرح برون‌سپاری رمزگذاری کارآمد مبتنی بر ابطال کاربر و ابطال ویژگی برای اینترنت اشیاء با استفاده از محاسبات مه ارائه می‌دهد. در [۲۰]، نویسندگان طرح‌های رمزگذاری مبتنی بر هویت فازی[4] اصلاح‌شده را پیشنهاد می‌دهند که از عملیات زوج‌نگار کمتری در مقایسه با طرح رمزگذاری مبتنی بر هویت فازی اصلی استفاده می‌کنند. طرح رمزگذاری مبتنی بر هویت فازی یک مورد خاص از رمزنگاری ویژگی مبنا است که خط‌مشی دسترسی به جای درخت دسترسی از یک دروازه آستانه ساده استفاده می‌نماید. در این طرح، یک مفهوم امنیتی جدید به نام امنیت انتخابی مشروط ۲[5] معرفی می‌شود که از مفهوم امنیتی انتخابی قوی تر است. همچنین در [۲۰] دو طرح رمزگذاری ویژگی مبنا مبتنی بر خط‌مشی کلید[6] پیشنهاد شده است که از عملیات زوج نگار کمتری در مقایسه با طرح‌های مشابه قبلی استفاده می‌کنند. در این طرح، عملیات سنگین مانند ضرب اسکالر در یک نقطه منحنی، توان و زوج نگار برون‌سپاری می‌شوند تا دستگاه‌های اینترنت اشیا بتوانند با پیچیدگی‌ها کنار بیایند.

در [۲۱]، میائو و همکاران. یک سیستم جستجوی متن رمزی ریزدانه سبک‌وزن[7] با معماری محاسبات مه مبتنی بر خط‌مشی متن رمز و رمزگذاری قابل‌جستجو[8] ارائه کرد. با انتقال محاسبات با سربار زیاد به گره مه، این طرح می‌تواند دسترسی به متن رمز را با کمک کلمات کلیدی با کارایی مناسب جستجو و کنترل کند. ژانگ و همکاران [۲۲] طرحی را با ساختار دسترسی پنهان در محاسبات ابری ارائه می‌دهد که می‌تواند حریم خصوصی کاربران را حفظ نماید و قابلیت‌های برون‌سپاری صحت‌سنجی شده و کنترل دسترسی ریزدانه را ارائه دهد. اینترنت وسایل نقلیه دارای رانندگی خودکار و ارتباطات نسل پنجم است که توجه بی‌سابقه‌ای را در دانشگاه و صنعت به خود جلب کرده است. رمزگشایی برون‌سپاری شده به مه در این طرح‌ها همچنان از محاسبات سریالی با سرعت پایین استفاده می‌کند و تجربه کاربری ضعیفی را ایجاد می‌کند؛ بنابراین، فنگ و همکاران [۲۳] یک مدل رمزگشایی برون‌سپاری شده موازی هوشمند لبه[9] برای اینترنت وسایل نقلیه پیشنهاد کردند. نویسندگان [۱۱] ترکیبی از الگوریتم‌های رمزگذاری متقارن و نامتقارن سبک‌وزن را بر اساس رمزگذاری مجدد پراکسی برای افزایش امنیت داده‌ها با کمک محاسبات مه در اکوسیستم اینترنت اشیاء پیشنهاد کرد. سیستم‌های پرونده پزشکی الکترونیکی[10]، کارایی خدمات پزشکی را افزایش می‌دهد، عملکرد منابع انسانی را بهبود می‌بخشد و تجویز دارو را دقیق‌تر می‌کند. باتوجه‌به حساسیت سوابق پزشکی، مسائل امنیتی در سیستم‌های اشتراک از اهمیت بالایی برخوردار است. طرح [۲۴] یک کنترل دسترسی سبک‌وزن برای به‌اشتراک‌گذاری سیستم‌های پرونده الکترونیک پزشکی در رایانش ابری با همکاری محاسبات مه پیشنهاد کرد. در [۲۵]، مدل استاندارد برای خط‌مشی دسترسی بر اساس مدل اشتراک‌گذاری راز خطی تعریف شد. این مدل نسبت به خط‌مشی دسترسی مبتنی بر درخت، عمومی‌تر است و عملکرد مطلوبی دارد. این ساختار مبتنی بر ماتریس تولید سهم است.

لی و همکاران [۱۹] طرحی را ارائه کردند که ابطال ویژگی و ابطال کاربر هم‌زمان را با استفاده از درخت باینری کِک[11] و محاسبات مه اجرا می‌کرد. همچنین سربار به‌روزرسانی متن رمز با جداسازی اطلاعات سرصفحه[12] از آن کاهش می‌یابد. سارما و همکاران [۲۶] طرحی به نام پک‌فیت[13] را با کمک محاسبات مه معرفی کردند که در برابر سپردن کلید مقاوم است. به‌عبارت‌دیگر، هیچ مرجعی به‌تنهایی نمی‌تواند متن رمز را رمزگشایی کند. آنها از مکانیزم ابطال ویژگی استفاده می‌کنند که فقط عناصر ابطال شده را بروز می‌کند، نه همه اجزای متن رمز را. سارما و همکاران در [۲]، طرحی به نام آرم‌فیت[14] ارائه کردند که از محاسبات مه استفاده می‌کرد. هدف آن ابطال ویژگی‌ها، ادغام[15] دو یا چند ویژگی، برون‌سپاری محاسبات سربار سنگین و اعطای دسترسی ویژه به کاربران خاص به طور کارآمد و هم‌زمان بود. مقاله [۲۷] یک طرح اشتراک داده شبکه هوشمند[16] مبتنی بر کنترل دسترسی ویژگی را بر اساس معماری محاسبات مه پیشنهاد می‌کند که دارای ابطال اختیارات امنیتی برای برآورده‌کردن الزامات امنیتی شبکه هوشمند است. در این طرح پارامترهای نسخه به بخشی از متن رمز و کلید محرمانه اضافه می‌شود و

[1] Identity-based encryption (IBE)
[3] Key escrow
[3] Matchmaking attribute-based encryption
[4] Fuzzy identity-based encryption (FIBE)
[5] Conditional Chosen Ciphertext Attack-2 (Conditional CCA-2)
[6] Key Policy-Attribute Based Encryption (KP-ABE)
[7] Lightweight Fine-Grained ciphertexts Search (LFGS)
[8] Searchable encryption (SE)
[9] ABEM-POD
[10] Electronic medical record (EMR)
[11] KEK tree
[12] Header
[13] PAC-FIT
[14] ARM-FIT
[15] Merging
[16] Smart Grid

امنیت را بهبود می‌بخشد. قابلیت‌های دیگر آن، رمزگشایی برون‌سپاری شده قابل‌تأیید، مراجع ویژگی چندگانه و ابطال کاربران است. مهم‌ترین اشکال طرح، هزینه زیاد به‌روزرسانی کلید در صورت ابطال مجوز است. برخلاف [۲۷]، در [۲۸] محاسبات سنگین در هر دو مرحله رمزگذاری و رمزگشایی به محاسبات مه و رایانش ابری برون‌سپاری شده است و نتایج پس از بازگرداندن به کاربران مورد بررسی و آزمون قرار می‌گیرند. در واقع، هرگاه دستگاه‌ها در اینترنت اشیاء دارای محدودیت منابع پردازشی باشند، بخشی از عملیات رمزگذاری یا رمزگشایی به سرورهای ابری یا محاسبات مه برون‌سپاری می‌شود. ممکن است محاسبات مه و رایانش ابری از الگوریتم‌های تعریف شده پیروی نکنند، فقط بخشی از محاسبات را اجرا کنند یا عمداً نتایج نادرستی را برگردانند. اگر این اتفاق بیفتد، مالک داده یا کاربر داده نمی‌تواند متوجه خطا شود و بخش بزرگی از محاسبات تحت تأثیر قرار می گیرد. بنابراین، لازم است نتایج رمزگذاری و رمزگشایی برون‌سپاری شده توسط کاربران صحت‌سنجی و تأیید گردند.

نویسندگان [۲۹] طرحی با نام RLT-CPABE را معرفی می‌کنند که امنیت داده‌ها را با ادغام مکان و زمان در فرایند رمزگذاری و رمزگشایی بهبود می‌بخشد. طرح از یک تابع اشتقاق محدوده واحد[1] برای پیاده‌سازی مقایسه محدوده زمانی و تکنیک رمزگذاری مجدد برای جاسازی زمان جاری در متن رمز استفاده می‌کند. از دیگر قابلیت‌های آن می‌توان به پشتیبانی مؤثر از ویژگی‌های متنی ثابت (ویژگی‌های عادی) و پویا (زمان و مکان)، ابطال کاربر و برون‌سپاری رمزگشایی به سرورهای مه اشاره نمود. نویسندگان در مقاله [۳۰]، یک طرح اشتراک‌گذاری سبک‌وزن و کارآمد برای حفظ حریم خصوصی پرونده‌های پزشکی الکترونیکی، بر اساس فناوری‌های اینترنت اشیاء، محاسبات مه و زنجیره قالب پیشنهاد کردند. علاوه بر این، قراردادهای هوشمندی[2] را برای پشتیبانی از پرس‌وجوهای متن رمز از طریق فهرست ذخیره‌شده، احراز هویت کاربر و قابلیت ممیزی[3] توسعه دادند. در مقاله [۳۱]، نویسندگان یک تکنیک به‌اشتراک‌گذاری داده چند مرجع امن و ترکیبی را برای یک سیستم مدیریت هوشمند بیمارستان[4] با رمزنگاری ویژگی مبنا، رمزگذاری بلو فیش[5] و امضای دیجیتال BLS[6] پیشنهاد شده است. در این طرح، داده‌های پزشکی در سرورهای مه و سرورهای ابری ذخیره و از احراز هویت چندگانه برای جلوگیری از فریب استفاده می‌شود. در مقاله [۳۲]، طرح SHARE-ABE پیشنهاد می‌شود که دارای قابلیت‌های همکاری[7] بین کاربران یک گروه و بهره‌گیری از خط‌مشی دسترسی پنهان[8] با معرفی ویژگی‌های نادرست[9]است. به‌عبارت‌دیگر، یک ویژگی همکاری تعریف می‌شود تا به کاربران درون یک گروه اجازه داده شود تا ویژگی‌های خود را درحالی‌که خط‌مشی دسترسی را برآورده می‌کنند ترکیب نمایند. علاوه بر این، از یک پروکسی برای افزودن ویژگی‌های نادرست به خط‌مشی دسترسی استفاده می‌شود تا کاربران مخرب نتوانند ویژگی‌های واقعی را حدس بزنند. همچنین فرایند رمزگشایی به سرورهای مه برون‌سپاری می‌شود.

در [۳۳] یک طرح رمزگذاری پخش ویژگی مبنا چند مرجع[10] پیشنهاد می‌شود که با تنظیم چند مرجع، مشکل سپردن کلید را حل می‌کند و از محدودیت‌های پهنای باند جلوگیری می‌نماید؛ بنابراین، چندین مقام به طور مشترک توزیع ویژگی‌ها را در طول فرایند تولید کلید مدیریت می‌کنند. به‌علاوه فرایند رمزگشایی به گره مه برون‌سپاری می‌شود. در [۳۴] طرح SPMAC معرفی شده است که معماری آن همانند طرح قبلی، مبتنی بر مراجع چندگانه است. این طرح از ابطال کاربر و ویژگی پشتیبانی می‌کند و با مخفی‌سازی کامل خط‌مشی دسترسی، از حریم خصوصی کاربران حمایت می‌کند. یانگ و همکاران [۳۵] یک طرح غیرمتمرکز ارائه کردند. آنها از دو روش ابطال ویژگی دوره‌ای و ابطال ویژگی فوری به طور هم‌زمان استفاده کردند. آنها همچنین از روش برون‌سپاری اختیاری برای رمزگشایی استفاده کردند. علی‌زاده و همکاران در [۹] یک طرح کنترل دسترسی رمزنگاری ویژگی مبنا ارائه کردند که می‌تواند در سیستم اعداد مانده‌ای پیاده‌سازی شود و از محاسبات با سربار ناچیز به‌جای عملیات نمایی و زوج نگار دوخطی استفاده می‌کند. آنها همچنین یک ساختار دسترسی مبتنی بر سیستم اعداد مانده‌ای ارائه کرده‌اند که دارای قابلیت موازی‌سازی است و از توابع بازگشتی استفاده نمی‌کند. در [۳۶]، لو و همکاران طرحی را بر اساس فناوری زنجیره قالب و رمزگذاری مجدد پراکسی ارائه کردند که دارای ویژگی‌های ابطال ویژگی، جستجوی کلمه کلیدی و ردیابی ویژگی در کلید محرمانه است. بااین‌حال، دارای نقاط ضعفی مانند نشت اطلاعات محرمانه، راندمان اجماع کم و به‌روزرسانی پیچیده مجوز برای حفظ داده‌ها در پلتفرم‌های ابری است. رمزگذاری ویژگی مبنا مقاوم در برابر نشت[11]، یکی از روش‌های کارآمد برای مقابله با حملات کانال جانبی[12] است. از طریق حمله کانال جانبی، کاربران مخربی که از ماهیت فیزیکی عملیات رمزنگاری مانند زمان‌بندی، توان مصرفی و تشعشعات، استفاده مجدد از کلید محرمانه یا تصادفی بودن برخی از برنامه‌ها سوءاستفاده می‌کنند، می‌توانند برخی از اطلاعات مخفی را دریافت کنند [۳۷]. در [۳۸]، طرح کنترل دسترسی PRE-CPABE برای حل مشکلات زنجیره قالب ، به‌روزرسانی متن رمزنگاری شده و رمزگذاری متقارن انجام شده است. در [۳۹]، تلاشی برای مقابله با حملات ایداس[13]و ابطال کاربران مخرب با کمک زنجیره قالب، به‌روزرسانی متن رمز و رمزگذاری متقارن انجام شده است. هیچ یک از طرح‌های [۳۶-۳۹] از محاسبات مه

[1] Single range derivation function
[2] Smart contracts
[3] Auditability
[4] Smart hospital management systems (SHMS)
[5] Blowfish
[6] Boneh-Lynn-Sacham
[7] Collaboration
[8] Hidden access policy
[9] False attribute
[10] Multi-authority attribute-based broadcast encryption (MA-ABBE)
[11] Leakage-resilient
[12] Side-channel attack
[13] EDoS

استفاده نکرده‌اند. فوگکیا[1] و همکاران [۴۰] یک طرح کنترل دسترسی برای حفاظت از پرونده‌های الکترونیک سلامت[2] بر اساس فناوری زنجیره قالب و محاسبات مه پیشنهاد کردند. این طرح دارای قابلیت ابطال کاربر بر اساس مدل‌سازی مبتنی بر نمودار است. با درنظرگرفتن حفاظت از حریم خصوصی و انتقال امن داده‌های مشترک در شبکه‌های اجتماعی خودرویی[3]، رِن و همکاران [۴۱]، طرح کنترل دسترسی BFDAC مبتنی بر زنجیره قالب و محاسبات مه را پیشنهاد کردند. شبکه‌های اجتماعی خودرویی، خدمات متعددی مانند رانندگی ایمن، به‌اشتراک‌گذاری داده‌ها و مدیریت ترافیک را در اختیار مسافران، رانندگان و وسایل نقلیه قرار می‌دهند. طرح BFDAC از ردیابی و ابطال کاربر پشتیبانی می‌کند و کاربران می‌توانند داده‌های اشتراک‌گذاری شده ذخیره شده در ابر را نیز باطل کنند.

۴- ارزیابی قابلیت‌های طرح‌ها

طرح‌هایی که از معماری محاسبات مه بهره بردند و در بخش قبلی مورد بررسی قرار گرفتند را طبق جدول (۱) و جدول (۲) مقایسه می‌کنیم و از منظر قابلیت‌ها و ویژگی‌های طرح‌های کنترل دسترسی مبتنی بر CP-ABE نظیر ابطال ویژگی و ابطال کاربر، پنهان‌سازی خط‌مشی، مدل خط‌مشی دسترسی، عملیات زیربنایی، کاربرد طرح و سایر قابلیت‌های افزونه، آنها را مورد آنالیز قرار می‌دهیم. همان‌گونه که ملاحظه می‌شود قابلیت ابطال ویژگی و کاربر دارای اهمیت است و بسیاری از مقالات مانند [۲،۱۹،۲۶،۲۷،۲۹،۳۴،۴۰،۴۱،۴۲] هردو یا یکی از آنها را پیاده‌سازی نموده‌اند. متأسفانه سربار محاسباتی عملیات ابطال زیاد است. به طور کلی در ابطال ویژگی دو عمل انجام می‌شود. ۱- بروزرسانی کلید محرمانه کاربرانی که ویژگی‌های مشابه آنها ابطال نشده است و ۲- بروزرسانی متن رمز برای کاربرانی که ویژگی‌های مشابه آنها ابطال نشده است. در معماری مبتنی بر محاسبات مه و رایانش ابری، وظیفه بروزرسانی متن رمز بر عهده سروهای ابری است و به چند مدل انجام می‌شود. در مدل اول [۴۲] که دارای بیشترین سربار است کلیه پارامترهای متن رمز شامل پارامترهای وابسته به ویژگی‌ها و پارامترهای غیر وابسته به ویژگی‌ها بروزرسانی می‌شود. در این مدل ویژگی‌هایی که ابطال نیز نشده‌اند تغییر می‌کنند. علاوه بر این به دلیل تغییر اجزای محرمانه متن رمز توسط سرور ابری، امنیت ابطال طرح کاهش می‌یابد. در مدل دوم [۲،۲۶] تنها ویژگی‌هایی که برای برخی کاربران ابطال شده است بروزرسانی می‌شود و در نتیجه سربار عملیات ابطال ویژگی کاهش می‌یابد. در مدل سوم [۷،۱۹] از روش رمزگذاری مجدد پراکسی برای بروز رسانی پارامترهای ویژگی‌های غیر ابطال شده متن رمز استفاده می‌شود و دارای امنیت مناسبی است. امکان دسترسی سرور ابری به پارامترهای محرمانه متن رمز وجود نخواهد داشت. مقالات [۱۹،۲۷،۲۹،۳۴] دارای قابلیت ابطال کاربر هستند. در این مقالات به هر کاربر علاوه بر ویژگی‌ها، هویت یا شناسه‌ای منحصر بفرد نیز اعطا می‌شود

جدول (۱): مقایسه قابلیت‌های طرح‌های مبتنی بر محاسبات مه

مقاله	نام طرح	کاربرد خاص	سایر قابلیت‌ها
[۱]	-	VFC	پنهان‌سازی
[۲]	ARM-FIT	ندارد	ادغام ویژگی
[۹]	RNS-ABE	ندارد	ندارد
[۱۶]	IBBE-ABE	E-learning	IBBE
[۱۸]	MABE	ندارد	Matchmaking
[۱۹]	-	ندارد	ندارد
[۲۱]	LFGS	ندارد	- رمزگذاری قابل‌جستجو - به‌روزرسانی ویژگی
[۲۲]	-	ندارد	- صحت‌سنجی عملیاتِ برون‌سپاری شده - پنهان‌سازی
[۲۳]	ABEM-POD	IoV	محاسبات موازی
[۲۴]	-	EMR	KP-ABKS[4]
[۲۶]	PAC-FIT	ندارد	مقاوم با سپردن کلید
[۲۷]	-	Smart Grid	صحت‌سنجی عملیاتِ برون‌سپاری شده
[۲۹]	RLT-CPABE	ندارد	ویژگی‌های پویا مبتنی بر زمان و مکان
[۳۰]	-	EMR	- زنجیره قالب - توسعه قراردادهای هوشمند - ممیزی
[۳۱]	-	SHMS	امضای BLS
[۳۲]	SHARE-ABE	ندارد	- همکاری کاربران - پنهان‌سازی
[۲۹]	MA-ABBE	ندارد	رمزگذاری پخش
[۳۴]	SPMAC	ندارد	تکنیک توکن‌های وب JSON[5] - پنهان‌سازی
[۴۰]	-	EHR	- زنجیره قالب -رمزگذاری متقارن
[۴۱]	BFDAC	VSN	- زنجیره قالب - ردیابی کاربران

تا بتوان بر اساس آن دسترسی یک کاربر ابطال شود. چالش جدی آن است که بتوان طرحی با قابلیت ابطال ویژگی و کاربر ارائه نمود که تنها کاربران یا ویژگی‌های ابطال شده بروزرسانی گردند تا سربار محاسباتی کاهش یابد و وابستگی به تمامی کاربران نداشته باشد.

قابلیت دیگر، پنهان‌سازی خط‌مشی دسترسی در متن رمز است تا بتوان حریم خصوصی را برای کاربران داده حفظ نمود. در مقالات [۲۲،۳۲،۳۴] به این مهم توجه شده است. با توجه به آنکه خط‌مشی دسترسی در متن رمز جایگذاری می‌شود، لازم است تمهیدی اندیشه شود تا بدون تحمیل سربار محاسباتی زیاد آنرا رمزگذاری کرد و تنها کاربران مجاز امکان دسترسی به آنرا به صورت محدود و بدون افشای ویژگی‌هایی که دارا نمی‌باشند، داشته باشند.

[1] Fugkeaw
[2] Electronic Health Record (EHR)
[3] Vehicular social networks (VSN)

[2] Key-policy attribute-based keyword search encryption
[3] JavaScript Object Notation (JSON) web tokens technique

جدول (۲): مقایسه ویژگی‌های طرح‌های مبتنی بر محاسبات مه

مقاله	نام طرح	قابلیت ابطال	عملیات زیر بنایی	مرجع ویژگی	مدل خط‌مشی
[۱]	-	خیر	زوج نگار	یگانه	LSSS
[۲]	ARM-FIT	ویژگی	زوج نگار	یگانه	درخت
[۹]	RNS-ABE	خیر	RNS	یگانه	RNS
[۱۶]	IBBE-ABE	خیر	زوج نگار	یگانه	درخت
[۱۸]	MABE	خیر	زوج نگار	یگانه	LSSS
[۱۹]	-	ویژگی کاربر	زوج نگار	چندگانه	درخت
[۲۱]	LFGS	خیر	زوج نگار	یگانه	درخت
[۲۲]	-	خیر	زوج نگار	یگانه	LSSS
[۲۳]	ABEM-POD	خیر	زوج نگار	یگانه	درخت یا Lsss
[۲۴]	-	خیر	زوج نگار	یگانه	درخت
[۲۶]	PAC-FIT	ویژگی	زوج نگار	چندگانه	درخت
[۲۷]	-	ویژگی کاربر	زوج نگار	چندگانه	درخت
[۲۹]	RLT-CPABE	کاربر	زوج نگار	یگانه	درخت
[۳۰]	-	خیر	XOR	یگانه	-
[۳۱]	-	خیر	زوج نگار	چندگانه	AND-OR
[۳۲]	SHARE-ABE	خیر	زوج نگار	یگانه	درخت
[۲۹]	MA-ABBE	خیر	زوج نگار	چندگانه	درخت
[۳۴]	SPMAC	ویژگی کاربر	زوج نگار	چندگانه	LSSS
[۴۰]	-	کاربر	زوج نگار	یگانه	درخت
[۴۱]	BFDAC	کاربر	زوج نگار	چندگانه	LSSS

اکثریت قاطع طرح‌های CP-ABE از عملیات زیربنایی زوج نگار دوخطی استفاده می‌کنند. در این طرح‌ها باهدف کاهش سربار محاسباتی دستگاه‌های با منابع محدود پردازشی، بخشی از عملیات زوج نگار دوخطی به سرورهای مه یا سرورهای ابری برون‌سپاری می‌شود. برون‌سپاری محاسبات چالش‌های امنیتی و حفظ حریم خصوصی ایجاد می‌کند؛ بنابراین چالش مهمی که هنوز باقی‌مانده است، آن است که آیا می‌توان از عملیات زیربنایی ذاتاً سبک‌وزن بهره برد طوریکه نیاز به برون‌سپاری محاسبات به طور کامل مرتفع گردد. نویسندگان در [۸] تلاش نمودند این چالش را برطرف کنند. اما تنها توانستند مرحله رمزگشایی را ذاتاً سبک‌وزن سازند. در این طرح آنها از سیستم اعداد مانده‌ای بهره گرفتند و خط‌مشی دسترسی مختص به آنرا طراحی نمودند. یکی دیگر از قابلیت‌های ضروری صحت‌سنجی کلیه عملیات برون‌سپاری شده است که در [۲۲،۲۷] به آن توجه شده است. متأسفانه سربار محاسباتی به کاربران تحمیل می‌شود و لازم است در جهت کاهش آن در آینده تلاش نمود.

براین‌اساس، پیشنهاد می‌شود در آینده، محققین گرامی در حوزه بهبود قابلیت‌ها، کارایی و امنیت طرح‌های CP-ABE مبتنی بر معماری محاسبات مه پژوهش‌های جامع‌تری انجام داده و تلاش نمایند تا به کمک فناوری‌هایی نظیر زنجیره قالب و RNS، کارایی آنها را به طور ذاتی بهبود دهند.

۵- نتیجه

یکی از کاربردی‌ترین مدل‌های کنترل دسترسی که کمک به حفظ محرمانگی و حریم خصوصی کاربران و همچنین امنیت دستگاه‌ها و سنسورها در اینترنت اشیاء می‌کند، طرح‌های کنترل دسترسی رمزنگاری ویژگی مبنا است. مهم‌ترین و منعطف‌ترین مدل آن، طرح‌های رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز است. در این تحقیق به بررسی ویژگی‌ها و جزئیات معماری انواع طرح‌های پیشنهاد شده مبتنی بر خط‌مشی متن رمز مانند ریزدانه بودن، ساختار خط‌مشی دسترسی، ساختار مراجع ویژگی و عملیات زیربنایی آن پرداخته‌ایم. اخیراً به دلیل ماهیت عملیات زوج نگار دوخطی و محدودیت پردازشی و ذخیره‌سازی داده در بسیاری از دستگاه‌های متصل به اینترنت اشیاء، از محاسبات مه در طرح‌های مختلف بهره‌گیری شده است. باتوجه‌به اهمیت محاسبات مه در کاربردهای بلادرنگ و وابسته به مکان، به نظر می‌رسد طرح‌های مختلف مبتنی بر خط‌مشی متن رمز که از محاسبات مه بهره برده‌اند کاربردی‌تر هستند.

براین‌اساس در این تحقیق علاوه بر موارد فوق به بررسی قابلیت‌های کاربردی طرح‌های رمزنگاری ویژگی مبنا مبتنی بر خط‌مشی متن رمز نظیر ابطال ویژگی‌ها، ابطال کاربران، سپردن کلید، مخفی‌سازی خط‌مشی دسترسی تعبیه‌شده در متن رمز پرداخته‌ایم. به نظر می‌رسد تمامی طرح‌های مرور شده در کنار محسناتی که دارند، چالش‌ها و ایراداتی نیز دارند. عملیات زیربنایی آنها نظیر زوج نگار دوخطی و توان رسانی، دارای سربار بالای محاسباتی است و قابلیت‌هایی نظیر ابطال ویژگی‌ها، ابطال کاربران، سپردن کلید، عدم محرمانگی خط‌مشی دسترسی تعبیه‌شده در متن رمز و به‌کارگیری مرجع ویژگی یگانه که سبب کاهش مقیاس‌پذیری آن خواهد شد؛ دارای چالش است. باهدف رفع چالش‌های فوق، چندین راهکار توسط مقالات مختلف نظیر برون‌سپاری محاسبات زوج نگار دوخطی به محاسبات مه، استقرار مراجع ویژگیِ توزیع‌یافته و به‌کارگیری عملیاتی نظیر RNS و XOR بجای زوج نگار دوخطی موردتوجه قرار گرفته است.

مراجع

[1] T. Gan, Y. Liao, Y. Liang, Z. Zhou, and G. Zhang, "Partial policy hiding attribute-based encryption in vehicular fog computing," *Soft Computing,* vol. 25, pp. 10543-10559, 2021, doi: 10.1007/s00500-021-05996-8.

[2] R. Sarma and F. A. Barbhuiya, "A secure and efficient access control scheme with attribute revocation and merging capabilities for fog-enabled IoT," *Computers and Electrical Engineering,* vol. 104, p. 108449, 2022, doi: 10.1016/j.compeleceng.2022.108449.

[3] M. El-Hajj and P. Beune, "Lightweight public key infrastructure for the Internet of Things: A systematic literature review," Journal of Industrial Information Integration, p. 100670, 2024, doi: 10.1016/j.jii.2024.100670.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22-26, 2005. Proceedings 24*, 2005: Springer, pp. 457-473., doi: 10.1007/11426639_27.

[5] S. Alshehri and T. Almehmadi, "A secure fog-cloud architecture using attribute-based encryption for the medical internet of things (MIoT)," *International Journal of Advanced Computer Science and Applications,* vol. 12, no. 12, 2021, doi: 10.14569/IJACSA.2021.01212112.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*, 2007: IEEE, pp. 321-334., doi: 10.1109/SP.2007.11.

[7] J. Zhao, P. Zeng, and K.-K. R. Choo, "An efficient access control scheme with outsourcing and attribute revocation for fog-enabled E-health," *IEEE Access*, vol. 9, pp. 13789-13799 ,2021, doi: 10.1109/ACCESS.2021.3052247.

[8] P. Ananda Mohan, "Residue number systems: Theory and applications," *Basel: Birghauser, Mathematics*, 2016, doi: 10.1007/978-3-319-41385-3.

[9] M. A. Alizadeh, S. Jafarali Jassbi, A. Khademzadeh, and M. Haghparast, "Novel lightweight and fine-grained fast access control using RNS properties in fog computing," *Cluster Computing,* vol. 27, no. 3, pp. 3799-3817, 2024, doi: 10.1007/s10586-023-04169-6.

[10] R. Trabelsi, G. Fersi, and M. Jmaiel, "Access control in Internet of Things: A survey," *Computers & Security,* p. 103472, 2023, doi: 10.1016/j.cose.2023.103472.

[11] O. A. Khashan, "Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment," *IEEE Access,* vol. 8, pp. 66878-66887, 2020, doi: 10.1109/ACCESS.2020.2984317.

[12] Z. Guo, G. Wang, G. Zhang, Y. Li, and J. Ni, "A multifactor combined data sharing scheme for vehicular fog computing using blockchain," *IEEE Internet of Things Journal,* vol. 10, no. 22, pp. 20049-20064, 2023, doi: 10.1109/JIOT.2023.3282672.

[13] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Generation Computer Systems,* vol. 78, pp. 753-762, 2018, doi: 10.1016/j.future.2016.12.015.

[14] Q. Huang, Y. Yang, and M. Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing," *Future Generation Computer Systems,* vol. 72, pp. 239-249, 2017, doi: 10.1016/j.future.2016.09.021.

[15] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things," *IEEE Access,* vol. 5, pp. 12941-12950, 2017, doi: 10.1109/ACCESS.2017.2727054.

[16] A. B. Amor, M. Abid, and A. Meddeb, "Secure fog-based e-learning scheme," *IEEE Access,* vol. 8, pp. 31920-31933, 2020, doi: 10.1109/ACCESS.2020.2973325.

[17] Y. Mahi Gayathri and K. Rekha, "Comparative analysis of identity-based-broadcast encryption with attribute-based encryption for reduced storage cost of multi users in a public cloud," in AIP Conference Proceedings, 2024, vol. 2729, no. 1: AIP Publishing, doi: 10.1063/5.0168813.

[18] S. Xu *et al.*, "Match in my way: Fine-grained bilateral access control for secure cloud-fog computing," *IEEE Transactions on Dependable and Secure Computing,* vol. 19, no. 2, pp. 1064-1077, 2020, doi: 10.1109/TDSC.2020.3001557.

[19] L. Li, Z. Wang, and N. Li, "Efficient attribute-based encryption outsourcing scheme with user and attribute revocation for fog-enabled IoT," *IEEE Access,* vol. 8, pp. 176738-176749, 2020, doi: 10.1109/ACCESS.2020.3025140.

[20] M. Mahdavi, M. H. Tadayon, M. S. Haghighi, and Z. Ahmadian, "IoT-friendly, pre-computed and outsourced attribute based encryption," Future Generation Computer Systems, vol. 150, pp. 115-126, 2024, doi: 10.1016/j.future.2023.08.015.

[21] Y. Miao, J. Ma, X. Liu, J. Weng, H. Li, and H. Li, "Lightweight fine-grained search over encrypted data in fog computing," *IEEE Transactions on Services Computing,* vol. 12, no. 5, pp. 772-785, 2018, doi: 10.1109/TSC.2018.2823309.

[22] J. Zhang, Z. Cheng, X. Cheng, and B. Chen, "OAC-HAS: outsourced access control with hidden access structures in fog-enhanced IoT systems," *Connection Science,* vol. 33, no. 4, pp. 1060-1076, 2021, doi:10.1080/09540091.2020.1841096.

[23] C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv, and S. Mumtaz, "Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 11, pp. 13784-13795, 2020, doi: 10.1109/TVT.2020.3027568.

[24] A. Zhang, X. Wang, X. Ye, and X. Xie, "Lightweight and fine-grained access control for cloud–fog-based electronic medical record sharing systems," *International Journal of Communication Systems,* vol. 34, no. 13, p. e4909, 2021, doi: 10.1002/dac.4909.

[25] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *International workshop on public key cryptography*, 2011: Springer, pp. 53-70., doi: 10.1007/978-3-642-19379-8_4.

[26] R. Sarma, C. Kumar, and F. A. Barbhuiya, "PAC-FIT: An efficient privacy preserving access control scheme for fog-enabled IoT," *Sustainable Computing: Informatics and Systems,* vol. 30, p. 100527, 2021, doi: 10.1016/j.suscom.2021.100527.

[27] Z. Wu, R.-h. Shi, K. Li, and Y. Yang, "Attribute-based data access control scheme with secure revocation in fog computing for smart grid," Cluster Computing, vol. 25, no. 6, pp. 3899-3913, 2022, doi: 10.1007/s10586-022-03616-0.

[28] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "A secure and verifiable outsourced access control scheme in fog-cloud computing," Sensors, vol. 17, no. 7, p. 1695, 2017, doi: 10.3390/s17071695.

[29] K. Routray and P. Bera, "RLT-CPABE: Revocable Location and Time Aware Ciphertext Policy Attribute-Based Encryption," in *2022 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, 2022: IEEE, pp. 409-414, doi: 10.1109/ANTS56424.2022.10227786.

[30] S. Fugkeaw, L. Wirz, and L. Hak, "An efficient medical records access control with auditable outsourced encryption and decryption," in *2023 15th International Conference on Knowledge and Smart Technology (KST)*, 2023: IEEE, pp. 1-6, doi: 10.1109/KST57286.2023.10086904.

[31] G. Thushara and S. M. S. Bhanu, "A new hybrid encryption in fog–cloud environment for secure medical data-sharing," *Iran Journal of Computer Science,* vol. 6, no. 2, pp. 169-183, 2023, doi: 10.1007/s42044-022-00129-2.

[32] A. Saidi, O. Nouali, and A. Amira, "SHARE-ABE: an efficient and secure data sharing framework based on ciphertext-policy attribute-based encryption and Fog computing," *Cluster Computing,* vol. 25, no. 1, pp. 167-185, 2022, doi: 10.1007/s10586-021-03382-5.

[33] J. Chen, J. Niu, H. Lei, L. Lin, and Y. Ling, "Adaptively secure multi-authority attribute-based broadcast encryption

in fog computing," *Computer Networks,* vol. 232, p. 109844, 2023, doi: 10.1016/j.comnet.2023.109844.
[34] R. Ma and L. Zhang, "SPMAC: Secure and privacy-preserving multi-authority access control for fog-enabled IoT cloud storage," *Journal of Systems Architecture,* vol. 142, p. 102951, 2023, doi: 10.1016/j.sysarc.2023.102951.
[35] F. Yang, H. Cui, and J. Jing, "Decentralized Attribute-Based Access Control with Attribute Revocation and Outsourced Decryption," in *2023 15th International Conference on Computer Research and Development (ICCRD)*, 2023: IEEE, pp. 246-257, doi: 10.1109/ICCRD56364.2023.10080306.
[36] Y. Lu, T. Feng, C. Liu, and W. Zhang, "A Blockchain and CP-ABE Based Access Control Scheme with Fine-Grained Revocation of Attributes in Cloud Health," *CMC-COMPUTERS MATERIALS & CONTINUA,* vol. 78, no. 2, pp. 2787-2811, 2024, doi: 10.32604/cmc.2023.046106.
[37] L. Zhang and Y. Shang, "Leakage-resilient Attribute-based Encryption with CCA2 Security," Int. J. Netw. Secur., vol. 21, no. 5, pp. 819-827, 2019, doi: 10.6633/IJNS.201909 21(5).14.
[38] C. Ruan, C. Hu, X. Li, S. Deng, Z. Liu, and J. Yu, "A Revocable and Fair Outsourcing Attribute-Based Access Control Scheme in Metaverse," *IEEE Transactions on Consumer Electronics,* 2024, doi: 10.1109/TCE.2024.3377107.
[39] Q. Zhang, C. Xu, H. Zhong, C. Gu, and J. Cui, "Revocable and Efficient Blockchain-based Fine-grained Access Control against EDoS Attacks in Cloud Storage," *IEEE Transactions on Computers,* 2024, doi: 10.1109/TC.2024.3398502.
[40] S. Fugkeaw, R. P. Gupta, and K. Worapaluk, "Secure and Fine-grained Access Control with Optimized Revocation for Outsourced IoT EHRs With Adaptive Load-Sharing in Fog-Assisted Cloud Environment," *IEEE Access,* 2024, doi: 10.1109/ACCESS.2024.3412754.
[41] Y. Ren, C. Chen, M. Hu, G. Feng, and X. Zhang, "Bfdac: A blockchain-based and fog computing-assisted data access control scheme in vehicular social networks," *IEEE Internet of Things Journal,* 2023, doi: 10.1109/JIOT.2023.3296906.
[42] S. Tu, M. Waqas, F. Huang, G. Abbas, and Z. H. Abbas, "A revocable and outsourced multi-authority attribute-based encryption scheme in fog computing," *Computer Networks,* vol. 195, p. 108196, 2021, doi: 10.1016/j.comnet.2021.108196.