A VERSATILE SECURITY FRAMEWORK USING BLOCKCHAIN TECHNOLOGY FOR FIFTH GENERATION COMMUNICATION NETWORKS

Sakthibalan P*, and Devarajan K
Assistant Professor, Department of ECE, Annamalai University, Chidambaram, Tamil Nadu, India
.E-Mail: balan1109@gmail.com
Assistant Professor, Department of ECE, Annamalai University, Chidambaram, Tamil Nadu, India
.E-Mail: devarajan_lecturer@yahoo.com

Abstract
The fifth-generation (5G) network assimilates terahertz bandwidth and machine type communication (MTC) for swift and reliable data transfer and information exchange. It incorporates sophisticated cloud, Internet of Things (IoT), and other software-defined architectures for providing scalable service support. However, due to the heterogeneous integration of devices and architectures, secure infrastructures need to become mandatory. In this article, a Blockchain-based Versatile Security Framework (BVSF) is introduced to provide robust and adaptable authentication and access control in the 5G environment. The proposed framework allocates blocks for user equipment (UE) authentication and resource access control in a parallel manner. The verification of security level between resources, infrastructures, and UEs aids in extending or attenuating blockchain services. Based on the different security level assessments, the UE requests are precisely mapped or reallocated to the resources, improving the response rate and the framework adaptability.

Keywords—5G, Access Control, Blockchain, Security Level, UE Authentication

Introduction
5G communication supports more wide area network (WAN) bands along with radios for wireless local area network (WLAN), FM services, and personal area network (PAN). An increase in users’ number will increase the demand for traffic in the network [1]. The prior aspect of 5G communication is the densification of the infrastructure. 5G cellular architecture is built by new techniques to overcome the spectral efficiency reduction, less data rate, and energy consumption of wireless communication systems [2].
In 5G security, the physical and logical layer security are loosely coupled; potential security threats like vulnerability and unknown attacks are considered [3]. The automatic detection and response are not provided by 5G security. The manual intervention in most of the security is provided in which applying security to large-scale complex 5G networks is difficult due to its efficiency and accuracy. An automated security mechanism is integrated into the 5G architecture for combatting different adversaries for performance enhancement [4, 5].

In 5G core network slicing, Slice isolation is used for proactively mitigates distributed denial of services attacks [6]. To mitigate distributed denial of services attacks is difficult. Hence, the 5G core network slicing is the first technique to evaluate the use of slice resource isolation to avoid these attacks. The service or the target network keeps selecting its resources and informs upstream routers (ISPs) to reduce the impact by blocking the traffic near the sources node [7, 8].

Related Works

In 5G networks, Wu et al. [9] proposed an authenticated key exchange protocol for multi-server architecture. Automatic encryption protocol tool ProVerif, information security analysis, and BAN logic are used to prove that the proposed protocol is secure. The proposed scheme's efficiency is better, and high security standards are achieved compared to existing schemes.

Maimo et al. [10] suggested a self-adaptive deep learning-based system in 5G networks for anomaly detection. The deep learning techniques analyze network traffic. Traffic fluctuation is managed, computing resources are optimized, and the analysis and detection process's performance and behavior are fine-tuned by automatically adapting the cyber-defense framework. Suitability and performance are determined by the proposed system for various traffic loads.

For cyber-Physical System (CPS) Over 5G network, Hussain et al. [11] considered deep learning-based DDoS attack detection. Malicious devices perform SMS spamming, signaling, silent call to avoid targeting calls, messaging, Internet, and CPSs operations are disrupted. The proposed framework achieves better accuracy for detecting the attack cell.

GRBC based network security function-placement scheme in SDS is implemented by Guan et al. [12] for 5G security. Group Routing Betweenness centrality (GRBC) is computed by adopting GRBC as a metric and by
introducing successive algorithms. The security functions' performance is improved in SDS systems under computer virus and worm control scenario in SDS through performance evaluation.

Secure modular smart contract platform is designed by Pustisek et al. [13] for multi-tenant 5G applications. Secure smart contracts are developed, key smart contract vulnerability is highlighted, and developer tools are used to support smart contract security. The per-contract smart contract tunnels are combined with user-based access control to reduce the vulnerabilities. Hybrid private, public blockchain networks obtain scalability, transaction cost optimization, performance, and security.

Li et al. [14] recommended a rule anomaly-free mechanism of security function chaining in 5G. With anomaly resolution configured rule management framework is implemented to avoid misconfigurations. The proposed mechanism's efficiency and availability are evaluated by performance evaluation to provide a solution for the security rule anomalies.

Efficient and secure service-oriented authentication supporting network slicing is proposed by Ni et al. [15] for 5G-enabled IoT. Based on service or slice types of accessing services, users can establish a 5G network connection and anonymous access to IoT services through selecting 5G infrastructure network slice by fog nodes. A privacy-preserving slice selection mechanism preserves configured slice type and accessing service type. The efficiency and feasibility of the proposed method are evaluated through its performance with the help of simulation.

For 5G-enabled vehicular networks, Cui et al. [16] considered reputation system-based lightweight message authentication framework and protocol. The proposed scheme is secure against the adaptively chosen message attack with the help of security analysis. Better performance is obtained by elliptic curve cryptosystem and batch authentication in the scheme's time compared to existing schemes.

Blockchain-Based Versatile Security Framework

The proposed BVSF aims at providing adaptable security measures for the 5G communication and information sharing. In this framework, blockchain technology is assimilated for heterogeneous and parallel security procedures. It includes both access control and authentication measures with the security level for combating different
attacks. A formal representation of the proposed framework is displayed in Fig. 1.

![Proposed Framework](image)

**Fig. 1 Proposed Framework**

As represented in Fig. 1, the end-users comprising user equipment (UE) communicate with the infrastructure units’ service. In this communication, the authentication based on shared credentials is monitored by the distributed ledgers. The access control and response validity between the infrastructure and resources are monitoring by the ledgers as a parallel security process. Let \( R \) and \( S \) denote the set of requests and service responses between the resources and end-users. The variables \( \delta_{UE-I} \) and \( \delta_{M-I} \) denotes the security level between UE and infrastructure and resource and infrastructure, respectively. Based on the optimal service response, the problem of non-versatility is defined using equation (1):

\[
\begin{align*}
\forall R = S = 1, & \delta_{UE-I} = \delta_{R-I} = \max \{ \delta_{UE-I} \cap \delta_{R-I} \} \\
\text{such that,} & \\
\{ N \}: \rightarrow M \text{ and all } M \leftarrow R \text{ Contrarily, if } N < M, \text{then } & \delta_{UE-I} = \delta_{M-I}(or) \delta_{UE-I} > \delta_{M-I} \text{ provided } S < 1 (or) (R - S)! = 0
\end{align*}
\]

In equation (1), the uneven transmission or the impact of adversaries form the irregularity in data/communication sessions. It is to be noted that the blockchain paradigm monitors and recommends security (access control and authentication parallel. Therefore, the security level needs to be balanced throughout the \( S \) dissemination for all the sessions. The authentication process is first provided by the \( N \) UE's mapped with \( M \) resources. In this authentication, UE's identifier (N_ID) is shared at the initial stage for providing authenticated sessions. The authentication session process is defined as

\[
A[session] = [N,ID]\|H(UE)\|H(I)]
A(communication) = A(session)\oplus Proc(d,k)
where proc \( (d, encryption) = Proc \ (d,p) \)
Proc \ (d, decryption) = Proc \ (d,\tau)
\]

In equation (2), the variables \( H(UE) \) and \( H(I) \) denotes the hash of UE and infrastructures, \( Proc \) is the procedures for encryption/decryption of the data \( d \) using public \( (P) \) and secret by \( (\tau) \). The function \( A(\cdot) \) denotes the
authentication of the session and communication for a given timestamp \( t_s \).
The \( t_s \) activated session is augmented in the blockchain system incrementing the session count by 1. This implies an open session in expecting responses through \( M \) allocating; However, the \( M \) retains some level of access for different requests, and the level is void if an adversary is detected. The failure in \( Prec \) (.) or \( A \) (session) or \( A \) (Communication) prevents \( N \) from accessing \( M \).

The access level is retained at a high rate such that \( \delta_{M-I} = 1 \) at the initial \( A \) (session) time. For this access grant interval for all \( R \) estimated as

\[
\alpha_t = \frac{s - \sum_{i=1}^{R} s_i}{(N-S)(R-S)} \quad \text{such that} \quad \delta_{UE-I} = \delta_{M-I} = 1
\]  

(3)

In equation (3), \( \alpha_t \) is the access grant interval; this interval either accommodates the entire session or discards the session at midst. Therefore, the access granting interval is \( \alpha_t \forall R \) regardless of \( \max \{ \delta_{UE-I} \cap \delta_{M-I} \} \). The access level is defined as in equation (4) for \( \alpha_t \) estimated in equation (3)

\[
\delta_{M-I} = \frac{A(\text{Communication})}{A(\text{session})} \forall t_s \iff \delta_{M-I} = 1
\]

such that

\[
A(\text{session}) = \alpha_t \text{ (or) } \text{Ver}(P,d,\gamma) \rightarrow \{0\} \| \{1\}
\]

where Ver\((P,d,\gamma) = \text{Ver}P,d,\text{sign}(\beta;d) \)

(4)

In equation (4), the variables \( \gamma \) denotes the secret key shared between \( I \) and \( N \). The function \( \text{Ver}(.) \) denotes the verification of \( d \) in \( A \) (communication) and sign(.) is the 'd' authenticating process. Similar to the process of access sharing, the security level between \( I \) and \( N \) is estimated as

\[
\delta_{UE-I} = \begin{cases} 
1, \text{if } \frac{S}{R} = 1 \text{ and } [\alpha_t = t_s] \\
0, \text{if } \frac{S}{R} < 0, \text{ and } [\alpha_t = 0] \\
0, \text{if } \frac{S}{R} < 0, \text{ but } [\alpha_t < t_s] \end{cases}
\]

(5)

In equation (5), the possible security level between \( I \) and \( UE \) is estimated. For all the \( \delta_{UE-I} \in \alpha_t \), the mapping of \( \delta_{M-I} \) is performed into \( t_s \). The blockchain system uses the matching process of the different security levels for ensuring its parallelism. The non-parallel/mismatching sequences are identified, and the blockchain support is either extended or reduced for secure sharing and communication. The process of authentication and access control from UE to \( M \) through \( I \) is presented in Fig.2.
The process of authentication and its accommodated security operates independently for different \( N \). However, the blockchain update is performed for \( N \) and \( M \) mapping based on the available \( \alpha_t \). The conditions in equation (5) are used to update the blockchain for providing further security or reducing its \( \alpha_t \). The termination of the session is also considered for versatile security. The versatility is based on scalable features for improving the adaptability of \( N \rightarrow M \) regardless of the availability. Thus, the blockchain update for the three conditions in equation (5) is verified in Table 1.

### Table 1 Blockchain Update Conditions and Output

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
<th>Assessment</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \alpha_t = t_s )</td>
<td>The timestamp and access grant intervals are equal</td>
<td>The authentication and access control features are concurrent, achieving high responses</td>
<td>( R = S ) such that ( \forall {N} \rightarrow M, \delta_{UE-I} \cap \delta_{M-I} = 1 )</td>
</tr>
<tr>
<td>( \alpha_t &lt; t_s )</td>
<td>The granted time is less than the allocated time stamp. The time stamp is then reallocated for the available ( {N} \rightarrow M )</td>
<td>The authentication failure in ( A(communi) ) is observed due to the adversary. This means the blockchain mapping is not performed and hence ( \alpha_t ) is less</td>
<td>( S &lt; R \forall {N} \rightarrow M ) in ( \alpha_t ) and ( \delta_{UE-I} \cap \delta_{M-I} = 1 ) such that ( \delta_{UE-I}(o r) \delta_{M-I} = 1 )</td>
</tr>
</tbody>
</table>
The service provider ends the access grant time due to any sensed adverse behavior. The blockchain is updated for $\delta_{M-1}$ and $\delta_{UE-1}$ and the $\{N\} \rightarrow M$ is performed at $(t_s - \alpha_t)$ time.

∀ $R \in t_s$, $(S - R) \in t_s \rightarrow (t_s + 1)$ such that $(S - R)$ is provided for new $N$ if equation (3) is true.

The above conditions and the outputs are used for providing scalable security measures. The versatility of the security framework is augmented based on the above conditions observed in different $S$ times. The block count and its adaptability are verified throughout the $s$ process, wherein the first condition is assessed. In the different sequence of response, the session failure (∀ $\alpha_t = 0$) and response ratio (in $\alpha_t = t_s$ and $\alpha_t < t_s$) are periodically updated. For this purpose, $\{N\} \rightarrow M$ and equation (4) are validated, ensuring the requirements in equation (1) are satisfied. Thus, the security measure's versatility and its parallel administration help provide realistic 5G services combating different attacks.

**Results and Discussion**

This section briefs the proposed framework's performance assessment using adaptability factor, session failure ratio, processing time, and response rate metrics. The assessment is a comparative study with the existing GRBC [12] and PAFM[14] methods. In this assessment, 50 UE's are used to communicate with six service providers. A blockchain system generates ten blocks for providing parallel security measures. The maximum timestamp validity is set as 48s and is refreshed periodically.

**Adaptability Factor**

![Fig. 3 Adaptability Factor for # UE and # Blocks](image-url)
Fig. 3 illustrates the comparative analysis of the adaptability factor for different UEs and blocks. The blocks in the authentication and access control process rely on \(N \rightarrow M\) and \(t_s\). The changes in the \(\delta_{M \rightarrow I}\) and \(\delta_{UE \rightarrow I}\) provides a different level of security for varying \(N\). Therefore, the security solution (authentication and access control) for \(S\) and \((S - R)\) is either single/ mapped at different intervals increasing the blockchain adaptability. As the process is synchronous (i.e.), parallel security is administered, using the blocks, extending the support for different UE's.

**Session Failure**

![Fig. 4 Session Failure for # Blocks](image)

The session failure ratio for different blocks is presented in Fig.4. The data exchange session is authenticated at the initial stage using \(N_{ID}\) for \(t_s\). In this process, both encryption and decryption are performed for \(A(communication)\), and hence data integrity is verified. The \(A(Session)\) is administered using blockchain for scalable and seamless integrity, ensuring successful \(S\). Therefore, the authentication and access control processes are updated by validating \(\delta_{M \rightarrow I} = \delta_{UE \rightarrow I}\) for all \(A(communication)\). In all the data exchanges process the conditions \(\alpha_t < t_s\) and \(\alpha_t = 0\) from \(\alpha_t = t_s\) are examined for improving \(S\). This helps to reduce the session failure regardless of the \(N\).

**Processing Time**

![Fig. 5 Processing Time for # UE](image)

The processing time varies for different UEs in multiple sessions. The processing time is high if \((S - R)\) is observed wherein the new mapping is performed. The available \(M\) is distributed for both available and overloaded \(R\). In the cases, authentication for \(R\) and access control for \(M\) is provided in all the session. The processing time for reallocation and response increases in \(\alpha_t = 0\) and \(\alpha_t < t_s\). Other than these instances, the processing time is less, besides the concurrency.
(parallel) in authentication and access control using different blocks stains the processing time (Refer to Fig. 5.)

**Response Rate**

![Fig. 6 Response Rate for # UE and # Blocks](image)

The proposed framework achieves a high response rate for different UEs and blocks, as represented in Fig. 6. The session failure ratio is less in the proposed framework, achieving high $S$. Besides $R$, $\alpha_t = t_s$ and $(S - R)$ $\alpha_t < t_s$ is differentiated for all sessions. Therefore, the $\delta_{UE-I}$ and $\delta_{M-I}$ is independently assessed for all the UE's and $M$. The session is authenticated in $t_s$ providing a better response rate. The blockchain update is provided for all the sessions improving the $S/R$ regardless of the UE's. The comparative study's performance results are tabulated in Tables 2 and 3 for # UEs and # blocks.

**Table 2 Performance Results for # UEs**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>GRBC</th>
<th>PAFM</th>
<th>BVSF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptability Factor</td>
<td>0.77</td>
<td>0.81</td>
<td>0.864</td>
</tr>
<tr>
<td>Processing Time (ms)</td>
<td>104.81</td>
<td>86.4</td>
<td>62.765</td>
</tr>
<tr>
<td>Response Rate</td>
<td>0.79</td>
<td>0.81</td>
<td>0.842</td>
</tr>
</tbody>
</table>

For the # UEs, the proposed BVSF achieves a 7.4% high adaptability factor, 4.2% high response rate, and 11.45% less processing time.

**Table 3 Performance Results for # Blocks**

<table>
<thead>
<tr>
<th>Metrics</th>
<th>GRBC</th>
<th>PAFM</th>
<th>BVSF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adaptability Factor</td>
<td>0.8</td>
<td>0.87</td>
<td>0.98</td>
</tr>
<tr>
<td>Session Failure (%)</td>
<td>7.9</td>
<td>6.58</td>
<td>5.371</td>
</tr>
<tr>
<td>Response Rate</td>
<td>0.86</td>
<td>0.9</td>
<td>0.983</td>
</tr>
</tbody>
</table>

The proposed framework improves adaptability factor and response rate by 7.25% and 5.15%, reducing session failure by 3.74%.

**Conclusion**

This article proposed a blockchain-based versatile framework for providing scalable and adaptable security for the 5G communication network. The proposed framework provides UE authentication and resource access control in a parallel manner. Based on the UE credentials, authentication is granted, and the access level is determined based on different time stamps. The authentication and access control features are updated using different
ledgers of the blockchain technology. Therefore, the scalable and UE adaptability feature increases regardless of the available resources. The experimental analysis shows that the proposed framework achieves better adaptability and response rate, reducing session failure and processing time.

References


