Article

A Lightweight Trust-less Authentication Framework for Massive IoT Systems

Aitizaz Ali[1,†,‡], Irene Delgado Noya[2,3,‡] Ateeq Ur Rehman[4,†,‡], Mehmood Ahmed [5,‡], Aman Singh [2,6,†,‡], Divya Anand [2,7,‡],

1 School of Information Technology, Monash University, Malaysia
2 Higher Polytechnic School, Universidad Europea del Atlántico, C/Isabel Torres 21, 39011 Santander, Spain
3 Department of Project Management, Universidad Internacional Iberoamericana, Campeche 24560, Mexico
4 Department of Biomedical Engineering, Foundation University Islamabad, Pakistan
5 Department of Information Technology, The University of Haripur KPK, Pakistan
6 Faculty of Engineering, Universidade Internacional do Cuanza, Estrada Nacional 250, Bairro Kaluapanda, Cuito-Bié, Angola
7 School of Computer Science and Engineering, Lovely Professional University, Punjab-144411
* Correspondence: hashimali@awkum.edu.pk;
† kimonchin@ums.edu.my.
‡ These authors contributed equally to this work.

Abstract: Because of the improvement of sensory technologies, there is an explosion in the development of low-cost electronic systems to operate smart city environmental features. Computer-based solutions that improve the quality of practical services are becoming increasingly popular as the world becomes more urbanised. Most present research on decentralised IoT applications focuses on a particular vulnerability. In contrast, for IoT-enabled industrial applications, only a few mechanisms address the challenges of privacy and trust. In addition, the current plans are in a poor state of repair. such as decentralised mobile networks when time is of the importance, like long-term evolution (LTE-A) The following is an example: Because of its trust-awareness and seamless authentication, TABSAPP is able to address issues of privacy, security, and delivery ratio. The redesigned traffic arrangement and the proposed method both make advantage of this technique. TAB-SAPP is shown to be a viable solution through the usage of identity management. boosts the number of active users by delivering more packets, which results in more mobility.
Keywords: security; privacy; blockchain; smartcontracts; IoT; encryption; transaction

1. Introduction

Artificial Intelligence (AI), blockchain, and the Internet of Things (IoT) are just few of the computing technologies that make up Industry 4.0. (IoT). The Internet of Things (IoT) devices are connected to each other via a cyber-physical system. In order to keep an eye on the health of data-intensive applications in real time, predictive maintenance can be employed. Smart intelligence capabilities embedded into each programme can help policymakers find data-driven solutions to pressing concerns.

Based on the difficulties of Module-SIS and Module-LWE problems, we present a significantly more practical way for establishing knowledge of a short vector fulfilling A's "t mod q." For the time being, demonstrating that s's l8 norm is modest is sufficient as a workaround. Polynomial product of CRTpmq and s coefficients is equal to 0 and the CRTpmq "t mod Q" polynomial vector with CRT coefficient equal to the s coefficients, is a polynomial vector. Since CRT embedding is a must and these approaches can only naturally be extended to show the l8-norm, they are already quite good for practical use. The l2 norms of the coefficients of s can be shown to be small using a straightforward and efficient method that does not necessitate an equivocation with the l8 norm or a conversion to the CRT form. If r and s are polynomials, then the product of their coefficients can be used to find this coefficient of the inner product between r and s. All except one coefficient of the proof for the modulo q inner product of two vectors is hidden using a polynomial product proof approach (or a vector with itself). The proof can be raised to Z instead of Zq using a low-cost, approximate range proof. A "interesting" inner product of vectors and polynomial products automorphism is enough to allow us to prove short norms using our methodologies.

The proliferation of industrial IoT applications and networking services has allowed for a tremendous increase in the number of connected devices. The application devices can capture real-time industrial data with a dedicated sensor unit [2]. Industrial advancement as well as technological guidance are behind this shift in the way systems interact with physical and logical things Centralized architecture is used to communicate real-time industrial data and evaluate the key components of IoT, including identity management. A single point of failure is feasible as a result of this common technique. A major issue with the Internet of Things (IoT) is the difficulty in maintaining and managing a large number of connected devices. System of networks can talk to interactivity through adaptive self-configuration. IoT applications can be commercialised over the 6G network. A fundamental component of the Internet of Things, the Wireless Sensor Network (WSN), gathers and transmits physical data using a range of heterogeneous models.
This article examines how computation can be offloaded to the physical layer in a blockchain-enabled Internet of Things (IoT) (PLS). MEC servers provide computational resources to help sensors complete their tasks after receiving task data from the BS (backend server). Gas providers are dissatisfied with current blockchain-based offloading schemes because of the lack of consideration of the gas cost for compute offloading. As a result of IRS-based wireless channels' time-varying features, it is impossible to estimate the data upload process's secrecy rate with a constant value. Using gas-oriented computing offloading to reduce sensor dissatisfaction while simultaneously reducing overall power usage is explained in this research. It is possible to allocate computer resources via IRS-assisted PLS transmission with ergodic secrecy. As a result of simulations, the proposed solution uses less energy and ensures the node that pays more receives more. Gas is the most potent of all the fuels available...

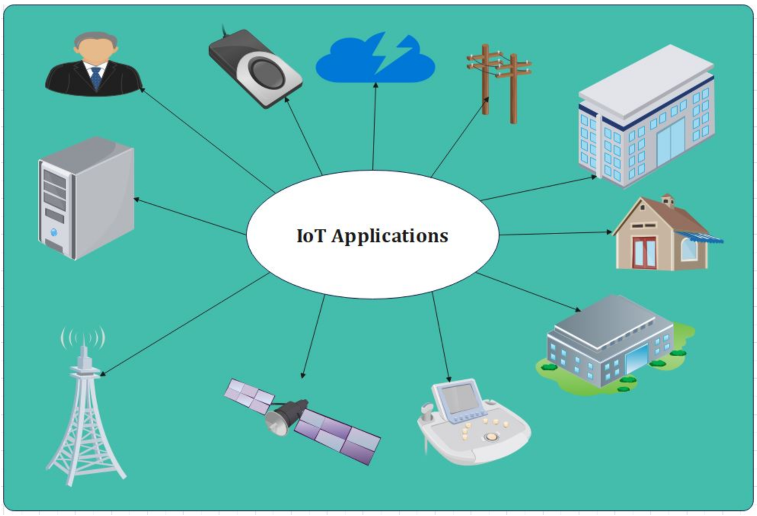

Figure 1. Applications of Internet of Things.

2. Background and Related Studies

Blockchain can be used to build trust and monitor node activity in IoT networks. Blockchain is challenging to integrate in IoT applications due to its high power consumption and job outsourcing. Several blockchain-based Internet of Things (IoT) applications have recently been created to address these concerns. These blocks can be used to delete old transactions and blocks from blockchains without jeopardising security. Pan et al. created an IoT resource management prototype using blockchain and smart contracts to securely record all IoT transactions [16]. Deploying smart contracts involves evaluating the source code, bytes of code, and execution histories, according to Angelo and Salzer [12]. This is how we test our computer traffic analysis deployment scenario. Wang et al. [13] investigated blockchain and smart contract applications in cloud storage. Pay-as-you-go is Tam et

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2022 doi:10.20944/preprints202205.0220.v1

alcar's business model. This technology's strengths are traceability and tamper-proof characteristics. [15] Yanqi et al. created a blockchain-based publisher-subscriber model. They designed their solution to assure data integrity in real-time IoT processing by balancing computational resources and workload. Liu et al. delegated computationally intensive PoW mining tasks to nearby edge servers in blockchain-enabled mobile IoT systems [18]. Chen et al. conducted additional research. Securing biometric data for patient authentication is a common issue. In particular, finger vein biometric data has been studied extensively. A strong verification mechanism with high levels of reliability, privacy, and security is required to better secure this data. Also, biometric data is difficult to replace, and any leakage of biometric data exposes users to serious threats, such as replay attacks employing stolen biometric data. This research offers a unique verification secure framework based on triplex blockchain-particle swarm optimization (PSO)-advanced encryption standard (AES) approaches for medical systems patients authentication. Discussion has three stages. First, presents a new hybrid modelpattern based on RFID and finger vein biometrics to boost randomness. It proposes a new merge method that combines RFID and finger vein characteristics in a random pattern. Second, the suggested verification safe framework is based on the CIA standard for telemedicine authentication using AES encryption, blockchain, and PSO in steganography. Finally, the proposed verification secure architecture was validated and evaluated. The combination of WSN functional activities with 6G network topologies allows us to test a wide range of IoT application deployment models. [4] Many IoT devices collect data using IPV6 across low-power wireless personal area networks and wearables (6LoWPAN) [5]. The Internet of Things influences authentication and key agreement mechanisms (IoT). We were able to keep user data confidential with AKA's help. [6]. Companies that use public cloud services and large-scale data storage systems have long prioritised client data protection. IMSS prefers machine authentication for public clouds.

recognising the value of reliable data in decision-making Batch processing may be required when working with huge data sets in the cloud. Even so, comparing the two seems impossible. To safeguard user passwords, Edward et al. [7] examined privacy laws and regulations. In real-time data communication with the Internet, dispersed mobility management rules and smart computers' activities are separated. Unlike real-time systems, cryptographic algorithms establish a public/private key pair. The cloudserver can read private cloud data by sharing a secret key [8]. Statista predicts 50 billion connected IoT devices by 2030. As a result, the market will increase rapidly in the future. Consistently protecting user privacy, blockchain-based trust might be used to seamlessly authenticate (TAB-SAPP). A smart design architecture is presented for spreading device connectivity over physical networks. The most widely used industrial automation standards are Zigbee, Z-Wave, and Bluetooth Low Energy (BLE). The blockchain's peer-to-peer nature allows IoT devices to connect. Decentralized IoT devices and consensus methods generate and store data in encrypted chain-like blocks, while smart contracts modify data and control the system. Blockchain-enabled IoT relies on a secure security paradigm (also known as IoT-EBT). This is possible because smart contracts retain and limit computing resources associated with a device's identification.

Different applications demand different levels of security, and resource scarcity plays a factor. Finding the best encryption technique for IoT medical data protection is essential. Electronic sensors capture medical data from patients and safely transmit it to the healthcare system. To avoid unwanted access or needless interruptions, trust and data privacy must be ensured from the start-sensors. Thus, data encryption from the start sensors is required, but due to restrictions in CPU complexity, battery consumption, and transmission bandwidth, using standard crypto-algorithms is impractical. Research on realistic lightweight encryption techniques for IoT medical systems. The study compares eight cryptographic algorithms in terms of memory usage and speed. The study determines the best candidate algorithm for the proposed health care system balancing the ideal requirement and future

 doi:10.20944/preprints202205.0220.v1

dangers.

Both parties must authenticate to use these services safely [32–35]. The server should require authentication to protect records from unauthorised users and ensure patient privacy (client side). Patient authentication is required to prevent server impersonation [32,36,37]. This proof-of-concept addresses emergency situations where a patient arrives unconscious at the hospital and needs to access information without providing an authorisation key. This issue requires safe biometric identification technologies as palm vein and iris [38–40]. In addition to providing high levels of security, usability, and dependability, biometric technology authentication has grown in popularity [39]. For example, the finger vein (FV) biometric is highly secure. Most modern authentication systems save biometric patterns in a database. Authentication extracts this data as biological biometrics. Secure biometric authentication with FV will be more resistant to security breaches and impersonation attempts. The human FV is a physiological biometric used to identify people by their blood veins' morphological characteristics. Individuals and offenders (in legal situations) are identified using this new technology, which is more accurate than other biometric systems [53–55].

Assuring the accuracy of verification results with low cost, time, and error rates is our goal. However, previous research shows that the utility of FV biometrics is severely limited. Securing the FV data inside the verification system is difficult since security breaches or biometric data leaks pose major security threats. Using stolen biometric data, for example [54]. This issue impairs the verification system's reliability, preventing stakeholders from using it. For example, when a user wants to access cloud computing or IoT services [55], data can be intercepted between the client and server or inside the database where the biometric data is stored. Because biometrics are permanent [56] and cannot be changed once taken, a solution must be devised. In order to secure FV biometrics, many researchers have used uni- or multi-biometrics, which include FV biometrics as part of the verification system. These approaches are applied in two steps, as follows: To protect FV patterns, researchers are trying to extract trustworthy properties from FVs, which can be used to uniquely identify individuals. These exclusive properties from the FV junction sites and the an-gles between veins are used to build a unique key (biokey). This key is used to encrypt data patterns[55,57]. The observation matrix extracts patterns and features, which are then encrypted with a random key [54]. Some researchers employed multi-biometrics to add to existing features. These traits have been used to identify people (FV, retina and fingerprint).

Tsai and Lo created identity-based authentication with mobile devices, service providers, and trusted third parties. Mobile devices and service providers can securely communicate using long-term secret keys. It is less efficient than ours due to the usage of bilinear pairing. Fan et al. claim that no suitable approach exists to prevent vulnerabilities. There is a solution for [20]. Yang et al. [21] devised a safe cloud computing handover method. It has a secret session-key. A network gateway generates and distributes a secret key before use. Banerjee et al. [22] presented anonymous user authentication in multiserver settings. It secures the system with ID-based cryptography. Create an authentication system that protects user privacy while lowering computation and transmission overhead. [18] Currently, implementing privacy protection for edge networks is tough. Park et al. [24] developed new authentication procedures to avoid Xiong et al's attacks. [24] Elliptic curve and biometric cryptography. Unlike Park et al. [25], Wang et al..

3. Contribution

1. Digital applications (DApps) use a trust-aware security approach to increase security and privacy while connecting huge IoT services.

Table 1. Access Control type, scope, scale, privacy issues, real time data-set used and accuracy's of various occupancy techniques

Technique/Technology	Reference	Scope (Shape/Size)	Scale (Number of People)	Privacy Issues	Sampling Time	Accuracy
Access Control	[?]	NA	18	Yes	Yes	80%
	[21]	60	NA	Yes	Yes	80%
	[2]	250	NA	Yes	Yes	80%
	[51]	100	NA	Yes	NA	92%
	[50]	100	8	Yes	Yes	NA
Access Control Types	[?]	50	1	No	Yes	NA
	[?]	NA	1	No	NA	NA
	[?]	NA	14	No	yes	86%
	[6]	NA	1	No	Yes	75%
Framework	[30]	100	2	No	yes	NA
	[33]	NA	150	No	NA	90%
Security	[?]	50	1	Yes	yes	93%
	[?]	200	NA	Yes	yes	79%
	[30] 100	NA	Yes	No s	NA	
	[?]	50	6	Yes	No s	60%
	[32]	100	30	Yes	NA	91%
Data Storage	[30]	NA	45	Yes	Yes	70%
	[31]	NA	4	No	Yes	80%
	[32]	100	4	No	Yes	NA
	[36]	40	9	No	Yes	80%
	[35]	200	23	No	NA	NA
	[36]	100	1	No	NA	70%
	[37]	50	3	No	Yes	80%
	[38]	150	3	No	Yes %	
	[39]	NA	3	No	Yes	73%
Efficiency	[40]	NA	72	No	NA	55%
	[40]	100	41	No	No	86%
	[41]	200	10	No	No	NA
	[42]	NA	NA	No	No	91%

 doi:10.20944/preprints202205.0220.v1

2. The sensing units generate industrial data across a dedicated network to concentrate the application service structure.
3. The network architecture connects to a variety of trustworthy IoT devices to meet 6Gen enabled IoT requirements.
4. The DApp's functions are enhanced with individual data such as biometric, video, and speech. DApp standardises smart intelligence by combining sensors, mobile networks, cloud resources, and service agents.
5. Edge computing is critical in 6G networks to reduce latencies [10].

4. Methodology

4.1. Proposed Algo

Algorithm 1 Attribute Based Signing Algorithm

Input: Initiate Master public key Ppub-s of domain, system parameters of domain, message M_0, e's identity I_{De}, and digital signature (h_0, S_0)

Output: Result of verification: pass or fail

Convert the Value of h_0 to int
if $h_0 \in [1, N \times 1]$ Not $\leq$, the verif fails
Compt Value t = g h_0 in G^T
Compt ω= H_2(h—δ, N)
Compt $\delta = (r \times h)$ mod N; if l = 0, move to sage 2)
Compt α = H1(IDe——hid, N)
Compt Value P = $[h_1]P_2 + P_{\text{pub-s}}$ in G2
Compt Value u = e(S_0, P) in G^T
Compt $w_0 = u \cdot t$ in G^T
convt the Value of w_0 to a bit string
Compt int $h_2 = H_2(M_0$——w_0, N)
if $h_2 = h_0$ holds, the verification
Otherwise, the verification fails
End Compt
Ret O
End Procedure

Algorithm 2 Algorithm Method Evaluation

Enhance Manifold Analysis Evaluation of both the PHR end
SelectPHR device for comm
Get acquisition, hash, electronic medical records (EMR) or PHR
Extract EMRFromRepository from EMR (EMR name)
PHR, valid SHA256 checkHash (PHR, hash)
if EMR or PHR, valid is true, then
Get the Connect Length using Connect length (Connect)
Generate Indications(Connect length) Generate Indications(Connect length)
F Blockchain transaction addAnalysis(i, indications)
deleteLocalEMR,PHR
end if (EMR,PHR)
end
end

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2022 doi:10.20944/preprints202205.0220.v1

Algorithm 3 Homomorphic Encryption

Public Key
T ← 0 indexed by keywords W
Choose key K_S for P_{R_F}
Choose keys $K_X, K_I, K_Z for P_{R_F} F_p$ *p and parse DB as $(id_i, W_{id_i})d_i = 1$ ← N ← F (KS , w)
id ∈ DB(w) d_o c ← 1 $x_{i_d} \leftarrow F_p(K_I, i_d), z \leftarrow F_p(K_Z, w||c)$
$y \leftarrow x_{i_{d_z}} - 1e \leftarrow E_{n_c}(K_e, i_d)$.
$x_{t_{a_g}} \leftarrow gF_p(K_X, w)x_{i_d} and X_{S_{e_t}} \leftarrow X_{S_{e_t}} U x_{t_{a_g}}$ (y, e) to t and c ← c + 1
[w] ← t

$(T_{S_{e_t}}, K_T) \leftarrow T_{S_{e_t}}.Setup(T)$
let $E_{D_B} = (T_{S_{e_t}}, X_{S_{e_t}})$
return $E_{D_B}, K = (K_S, K_X, K_I, K_Z, K_T)$
Token Generation $(q('w), K)$
Client's input is K and query $q('w = (w_1, ..., w_n))$
Compute $stag \leftarrow T_Set.Get_Tag(K_T, w_1)$
Client sends stag to the server
c = 1, 2, . . . until the server stops i = 2, . . . , n
$x_{to_{k_{en[c,i]}}} \leftarrow gF_p(K_Z, w1||c)F_p(K_X, w_i)$

$x_{to_{k_{en[c]}}} \leftarrow (x_{to_{k_{en[c,2]}}}, ..., x_{token[c,n]})$

$Tokq \leftarrow (s_{t_{a_g}}, x_{to_{k_{en}}})$
return T okq
Searching Technique
$E_{R_{e_s}} \leftarrow$
$t \leftarrow T_Set_(Retrieve)(T_{S_{e_t}}, stag)$
Verification result: succeed or fail

Algorithm 4 Initialization Algorithm

Initialize $T \longleftarrow \phi$ indexed by keywords W
Select key K_S for P_{RF} F
Select keys K_X, K_I, K_Z for P_{RF} F_p with range
$Z * p$ and parse D_B as $(id_i, W_i\, d_i)d_i = 1$
Initialize $t \longleftarrow ...$; and let $K_e \longleftarrow F(K_S, w)$
for id belongs to $D_B(w)d_o$
Set a counter $c \longleftarrow 1$
Compute $x_{id} \longleftarrow F_p(K_I, i_d), z \longleftarrow F_p(K_Z, w||c)$
$y \longleftarrow x_{idz} - 1\, e \longleftarrow E_{nc}(K_e, i_d)$
Set $x_{tag} \longleftarrow g\, F_p(K_X, w)x_{id}$ and $X_{Set} \longleftarrow X_{Set}$ union x_{tag}
Append (y, e) to t and $c \longleftarrow c + 1$
end for
$T[w] \longleftarrow t$
end for
Set $(T_{Set}, K_T) \longleftarrow T_{Set}$ Setup(T)
Let $E_{DB} = (T_{Set}, X_{Set})$
return $E_{DB}, K = (K_S, K_X, K_I, K_Z, K_T)$
Token generation $(q(w), K)$
Client's input is K and query $q(w = (w_1, ..., w_n))$
Computes stag $\longleftarrow T_{Set}$ Get $Tag(K_T, w_1)$
Client sends s_{tag} to the server
for $c = 1, 2, ...$ until the server stops do
for $i = 2, ..., n$ do
$x_{token}[c, i] \longleftarrow g\, F_p(K_Z, w1||c)F_p(K_X, w_i)$
end for
$x_{token}[c] \longleftarrow (x_{token}[c, 2], ..., x_{token}[c, n])$
end for
$T_{okq} \longleftarrow (s_{tag}, x_{token})$
return T_{okq}
Searching technique
$E_{Res} \longleftarrow ...$
: $t \longleftarrow T_{Set_{(Retrieve)}}(T_{Set}, s_{tag})$

 doi:10.20944/preprints202205.0220.v1

4.2. System Model

An industrial automation authentication system that is both trustworthy and simple is the purpose of this section. Private keys can be tested for security using a multisig-compatible contract, ensuring that no one else has access. Industrial automation will create a pay-as-you-go intelligent approach to explore the computing processes of IoT gadgets. The TAB-SAPP system is depicted in Figure 1. A multisigcompatible contract examines all aspect of a transaction, from quality control to mechanical technique to decision-making. In order to make independent decisions, the intelligent model makes use of traffic patterns. An IoT device's fundamental operational operations are analysed by a smart contract in order to maximise overall system efficiency. Table II shows how scientists use the TAB-SAPP notation.

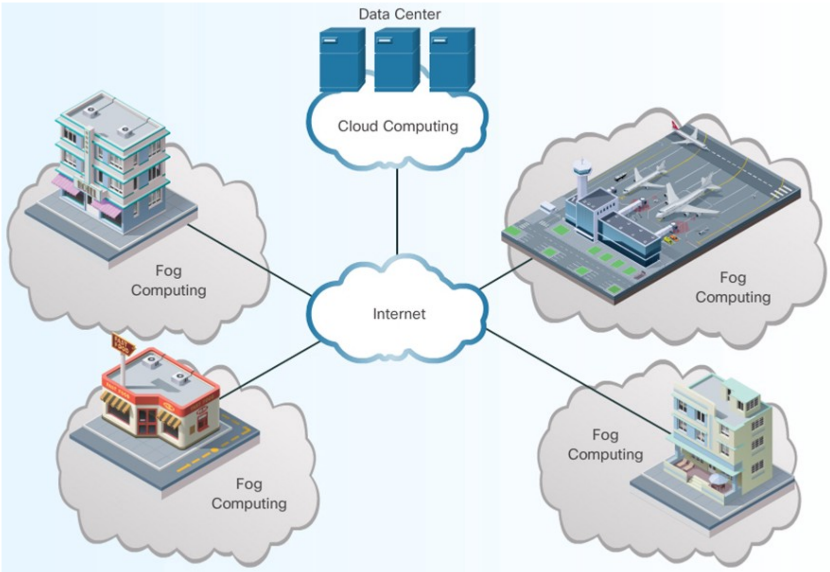

Figure 2. Application of Cloud computing .

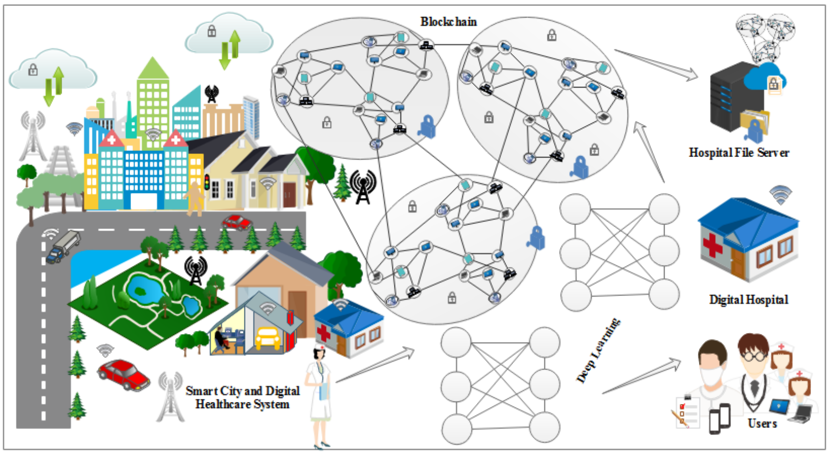

Figure 3. System Model Using healthcare Systems.

Components of communication include: An external owner account can access a billfold contract. A reliable transaction can address the different IoT devices scattered by automation. authorities. Automation and control experts are needed to distribute and manage large IoT devices. You can use an external owner account to warn consumers. Consumer-owned contracts are managed via a billfold. Control agreements can ensure a device's security. Consumers regularly use IoT devices to transact. Sending a Web3API transaction requires a contract state. Using a Billfold Contract, clients may securely access

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2022 doi:10.20944/preprints202205.0220.v1

industrial assets and register large IoT devices. Control contract: The control contract allows the public to inspect and approve the IoT device's worth. In the proposed TAB-SAPP, smart contracts handle whitelisting, IoT registration, IoT payment, key computation, and device operation. Consumer signature uses 256-bit Keccak hash to cope with external account (ECDSA). The control contract's private key connects the user, IoT device, and control contract. Here are the steps: In the first phase, an external owner account creates a whitelist. The control contract charges a fee to indicate consumer device access. Anyone who wants to verify a transaction on the blockchain pays a charge. The client and IoT device are linked to the external owner account in step two. Allows for consideration of consumer needs when fulfilling contractual responsibilities. After successful registration, the IoT gadget pays fees. TAB-SAPP smart contracts will handle whitelisting, registration, payment, and key computation. Encrypted elliptic curve signatures with Keccak hash (ECDSA). The control contract's private key addresses the consumer, IoT device, and control contract. Here are the steps: The contract organisation maintains and updates the whitelist using an external owner account. The consumer device control contract specifies the fee request. Using multisignature to verify a data transaction costs each party. To complete IoT registration, customers and devices must be linked to an external owner account. The contract organisation can accommodate client requests. The IoT gadget then handles the fee payment.

4.3. Elliptic Curve and Ring Signature Integration

List of Abbreviations			
Symbols	Purpose	Symbols	Purpose
Y	AF	H	Hash Algorithm
x	x-value	a	248
k	Constant	b	008
z	DZ	R	012
p	Prime	L	016
k	AD	R0	020
G	Bilinear Group	mod	024

$$y^2 \bmod q = (x^3 + ax + b) \bmod, q, \tag{1}$$

where a, b, x, and y belong to q and If a point P(x, y) satisfies the equation(1), then the point P(x, y) is a point on an elliptic curve, and the point Q(x, y) is the negative point of P(x, y) i.e. P=Q. Let points P(x1, y1) and Q(x2, y2) be points on the elliptic curves Eq (a, b) and P∗6 =Q, the line 'l' passes through the points P and Q, and intersects the elliptic curve at the point R0 = (x3, y), the points of R0 symmetrical about the x-axis are R=(x3, y3) and R=P+Q. The points on the elliptic curve Eq (a, b) and the infinite point O together form an additive cyclic group of prime order q as

$$G_q = (x, y) : a, b, x, y \text{ belong to } F_q, (x, y) \text{ belong to } F_q, (a, b). \tag{2}$$

$$k_P = P + P + ... + P(k \text{ belong to } Z_q), \tag{3}$$

$$((u_i + v_i) * G), \text{ if } i = S, \tag{4}$$

$$(u_i\, G + (v_i + w_i)) * p\, k_i, \text{ if } i =!S, \tag{5}$$

$$R_i = \sum (u_i + w_i) * H_0(p * k_i), \text{ if } i = s, \tag{6}$$

$$R_I = \sum u_i * H_0(p * k_i) + (v_i + w_i) * I_s \text{ if } i = s, \tag{7}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2022 doi:10.20944/preprints202205.0220.v1

$$h = H2(m||r), \tag{8}$$

where h is ..., $H2$ is ..., m is ..., and r is ... .

$$C_i = \sum H1(h, L_1, ..., L_n, R_1, ..., R_n) - \sum_{i=1}^{\infty} \frac{1}{n^s}, \tag{9}$$

$$D_{it} = \sum (u_i + v_i) c_i * s k_i, \tag{10}$$

$$D_{it} = \sum u_i \text{ if } i = s. \tag{11}$$

$$Y_i = d_i * G + c_i * p k_i, \tag{12}$$

$$i = d_i * H_0(p k_i) + c_i * I_s. \tag{13}$$

$$\sum_{ß=1}^{\infty} = H_1(h, Y_1, Y_2, ..., Y_n, K_1, K_2, ..., K_n), \tag{14}$$

$$\sum_{i=1}^{n} = H1(h, Y_1, Y_2, ..., Y_n, \delta_1, \delta, ..., \delta_n), \tag{15}$$

$$Y_i = d_i * G + c_i * p k_i = u_i * G + (v_i + w_i) * p k_i = L_i(, \tag{16}$$

$$Z_i = d_i * H_0(p k_i) + c_i * I_s = u_i * H_0(p k_i) + (v_i + w_i) * I_s = R_i, \tag{17}$$

When $i = s$, the conversions of (K_i) and (Z_i) are expressed as

$$K_i = d_i * G + c_i * p k_i, \tag{18}$$

and

$$Z_i = [(u_i + v_i) - c_i * s k_i] * G + c_i * p k_i, \tag{19}$$

respectively.

$$= u_i * G + v_i * G, \tag{20}$$

$$\delta_i = d_i * H0(p k_i) + c_i * I_s. \tag{21}$$

$$= [(u_i + v_i) - c_i * s k_i] * H0(p k_i) + c_i * s k_s * H0(p k_s). \tag{22}$$

$$= u_i * H0(p k_i) + v_i * H0(p k_i). \tag{23}$$

Therefore, according to the above relationship, the correctness of the ring signature scheme proposed in this paper is verified as

$$= H1(h, Y_1, Y_2, ..., Y_s, ..., Y_n, \delta_1, \delta_2, ..., \delta_s, ..., \delta_n), \tag{24}$$

$$= H1(h, L_1, L_2, ..., L_s, ..., L_n, R_1, R_2, ..., R_s, ..., R_n), \tag{25}$$

$$C_S = \sum_{i=1}^{n}, \tag{26}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2022 doi:10.20944/preprints202205.0220.v1

$$= \sum_{i=1}^{n} C_i, \tag{27}$$

Table 2. Simulation setup, configurations, and specifications

Parameters	Details
Dataset size	100 number of blocks + PHR
Hardware	GPU Enabled System
Software	Ethereum, Hyper-ledger Fabric
Parameters	Block Height, Number of blocks, No.Transac, No.PHR, Delay, signature creation
Performance Metric	Efficiency (Average percentage of Gas, No.packets, No.dead Nodes, No,Alive Nodes), security(Execution time of Policies) and Cost(Execution Time of Blocks),
Number of simulations	Number of Test performed on single data set.
Number of rounds or transactions	5000

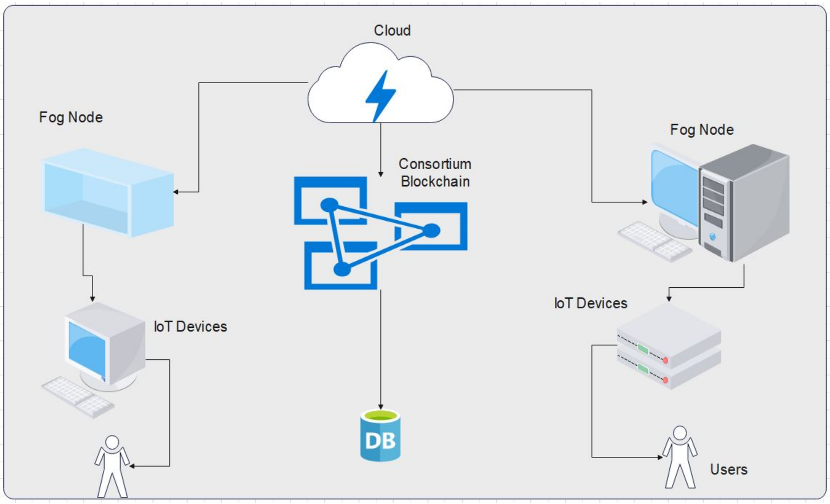

Figure 4. Proposed Framework.

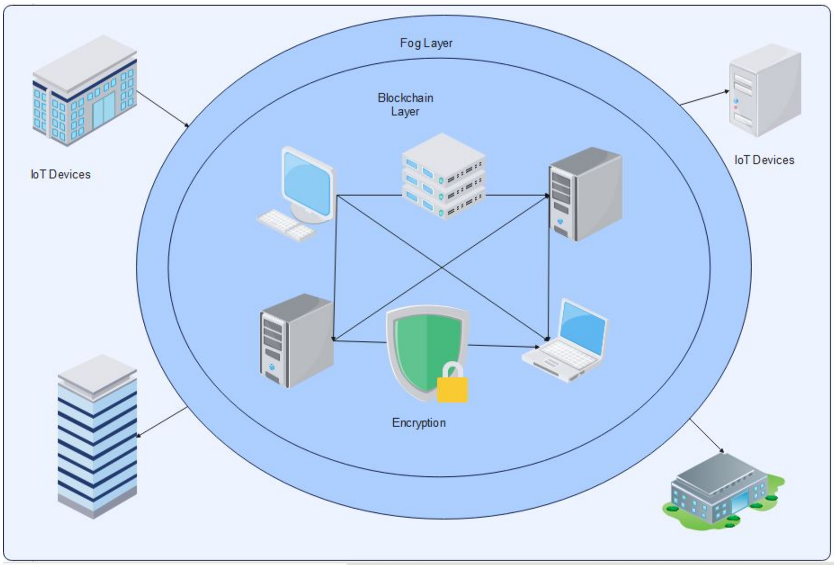

Figure 5. proposed System Architecture.

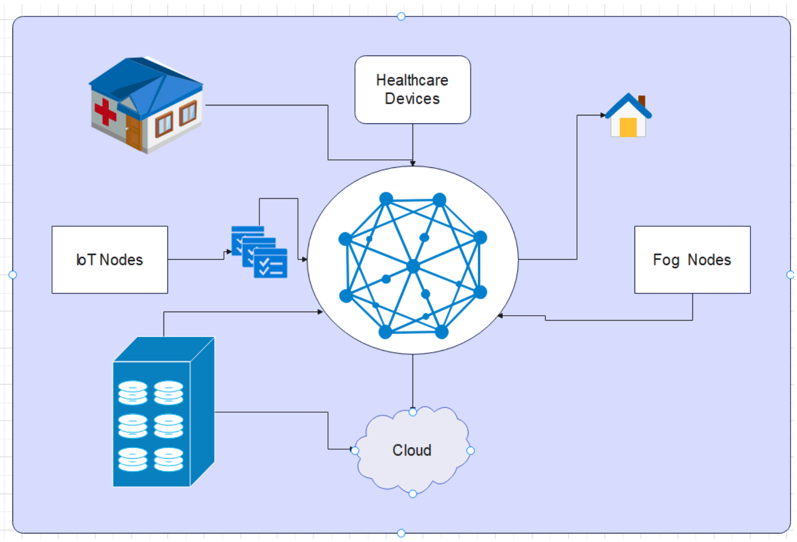

Figure 6. Data Flow through Proposed Network.

Table 3. This is a table caption. Tables should be placed in the main text near to the first time they are cited.

Serial No	Parameters	Description
Entry 1	Data	Data
Entry 2	Data	Data

Table 4. This is a wide table.

Title 1	Title 2	Title 3	Title 4
Entry 1	Data	Data	Data
Entry 2	Data	Data	Data [1]

[1] This is a table footnote.

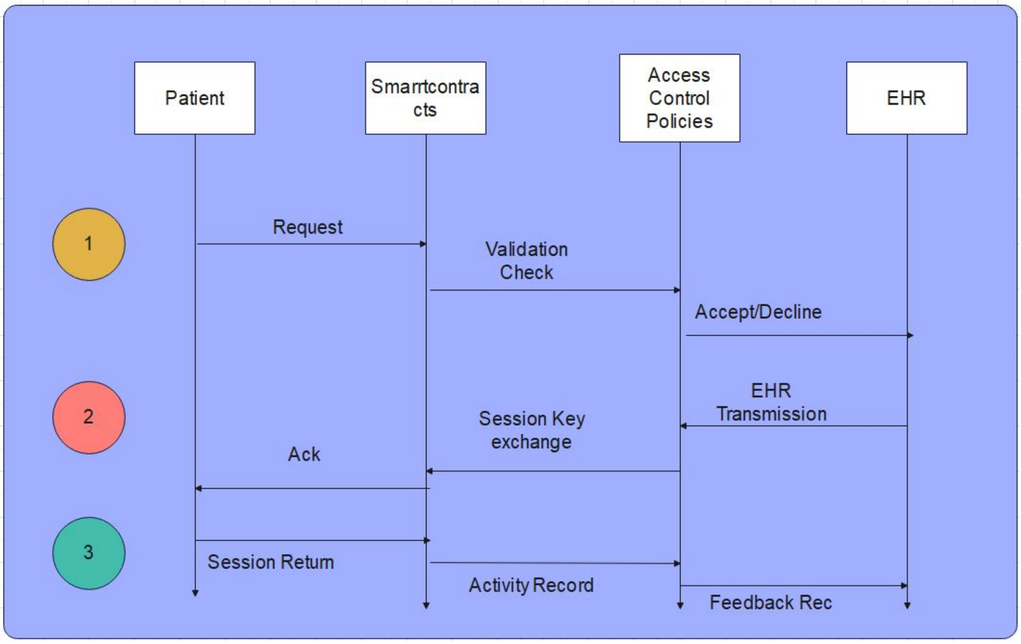

Figure 7. Timeline execution through Proposed Framework.

4.4. Mathematical Modeling

4.4.1. Phase 1: System Setup

Setup(α): Input security parameter (α)

$$let\ (G_1)\ and\ (G_2)\ be\ two\ multiplicative\ cyclic\ groups\ with\ generators\ p. \tag{28}$$

$$Assume\ (g_1),\ (g_2)\ are\ two\ generators\ of\ (G_1). \tag{29}$$

Let e : $(G_1) \prod (G_1) \implies (G_2)$ be an admissible bi linear map.The system randomly selects $\alpha, \beta \in$ Z ∗ p , computes g α 2 , g β 2 , g β (α1) .Select four hash functions H1 : 0, 1 ∗ → Z ∗ p

H2 : G_1 (Z ∗ p)

H3 : Z ∗ p → G2

H4 : G2 → 0, 1 ∗.

The system parameters PP = (p, e, g_1, g_2, g α 2 , g β 2 , g β (α) 1 , $G_1, G_2, H_1, H_2, H_3, H_4$)

Master secret key msk keeps secret msk = (a, B)

4.4.2. Encryption

The transaction was encrypted using attribute-based encryption techniques. We used ring signature instead of group signature or AES (Asymmetric Encryption System) for the key exchange. It protects against collusion assaults.

$$[(2+n)K+1]C_e x + (2K+1)C_m + (2K+1)C_m \tag{30}$$

$$\prod_{x=0}^{n} x - x_j/x_i - x_j. \tag{31}$$

4.4.3. Decryption

The recipient decrypts the message using both the public and private keys. A user with the appropriate attributes can decrypt the ciphertext. In the proposed framework, authorised users exchange keys via CA. The decryption time complexity equation is as follows: Where K is the number of certificate authorities, n is the message size, and C is the ciphertext.

$$[(n+1)K+1]C_p + nKC_e + [3+(2+n)K]C_m \tag{32}$$

 doi:10.20944/preprints202205.0220.v1

$$X = Qk \in ICe(C_2, D_k, u), Y = e(C_3, D_1k, u) \tag{33}$$

$$S_k = Q_ak, j \in A_kmeC_k, j, D_jk, u\delta ak, j, A\tilde{}j_m(0) \tag{34}$$

$$m = C_1X/YQk \in IC_S. \tag{35}$$

5. Results

In this section we present the simulations results carried out through this research paper. The data set were used which is publicly available from UNSW.

6. Experimental setup

The performance of our proposed framework was compared to benchmark models. We utilised a Raspberry Pi and Python. Moreover, Section 1 focuses on communication overhead in private information retrieval with varying appointment allocation mechanisms. Patients are charged a communication overhead (in bytes) while retrieving data from blockchain nodes. FIG. 8 depicts the communication overhead in private information retrieval, with several appointment allocation algorithms available in each cell. It can handle the required retrievals by storing in the B+-Tree indexing data structure. SHealth, MedRec, and ECC-Smart solution methods have higher communication overhead than the suggested architecture.

A communication overhead for retrieving private information from multiple blockchain nodes is shown in Fig. 9. Even if the number of blockchain nodes increases, the suggested framework scheme's communication overhead decreases because Redis cache-based indexing eliminates variables that impede retrieval of users' private information by service providers. How many blockchain nodes does the proposed strategy require to retrieve private information? The suggested approach is compared to the bench-marked (MBO)-SMS, (CB)-SMS, and ECC-SMS approaches in terms of communication overhead in private information retrieval with varying parking allotment in each cell and number of blockchain nodes accessible.

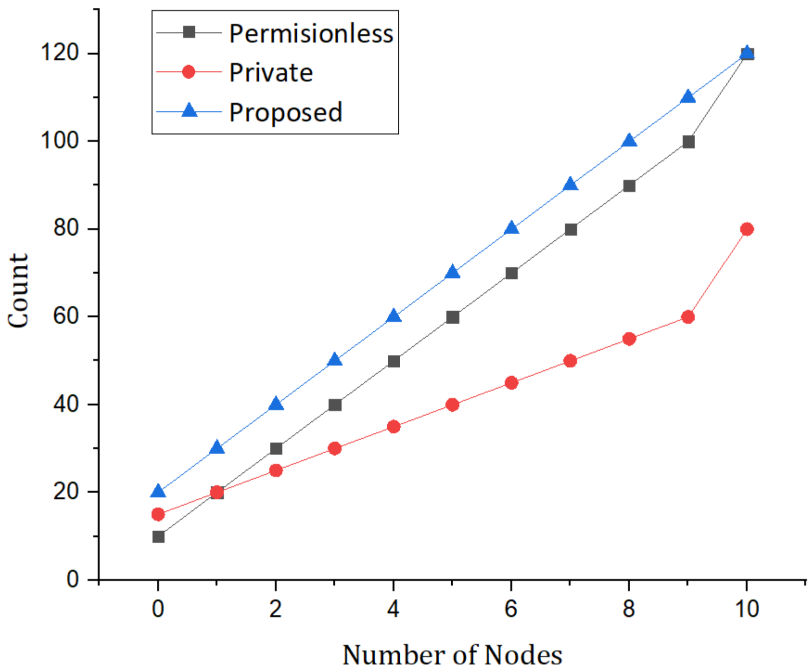

Figure 8. Simulations results based on number of nodes versus number of counts.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2022 doi:10.20944/preprints202205.0220.v1

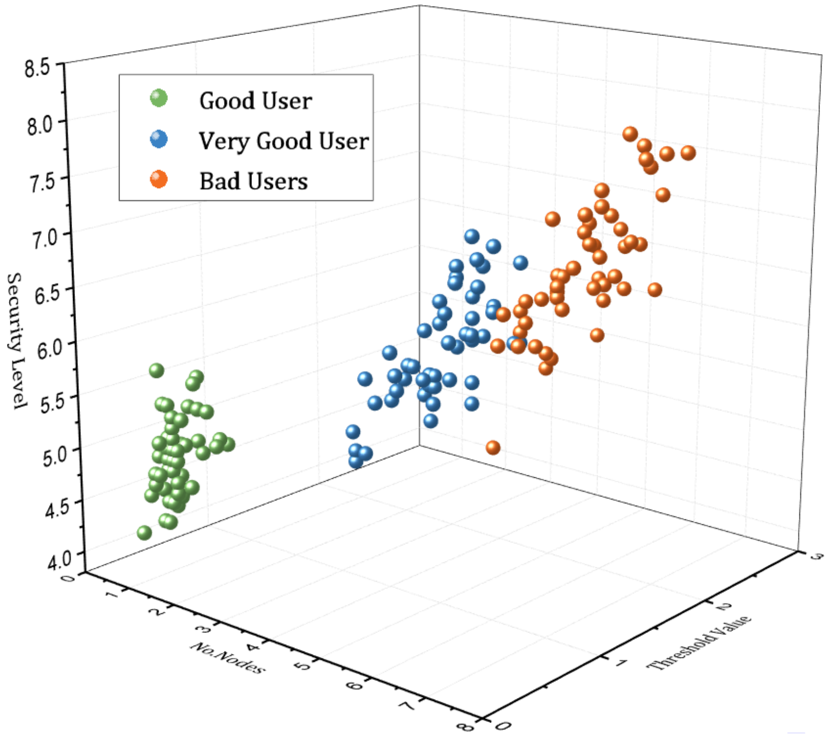

Figure 9. Classification of Users based on the behaviour and Interaction with the System Model.

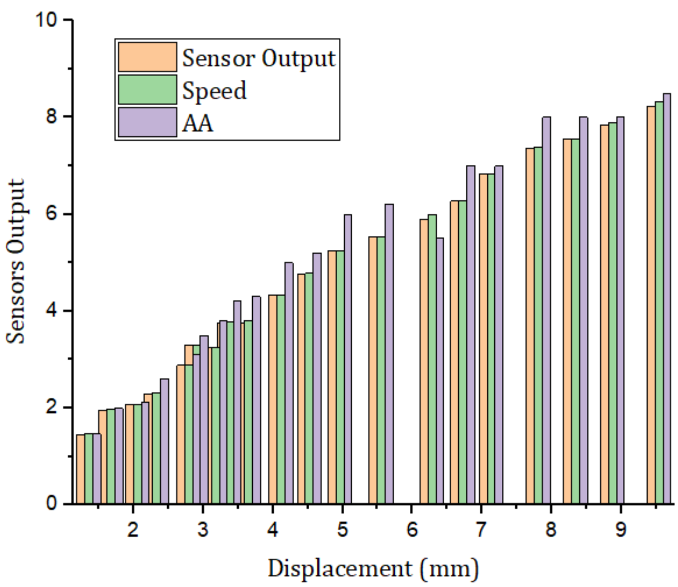

Figure 10. Simulations results based on the number of sensors output w.r.t number of nodes.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2022 doi:10.20944/preprints202205.0220.v1

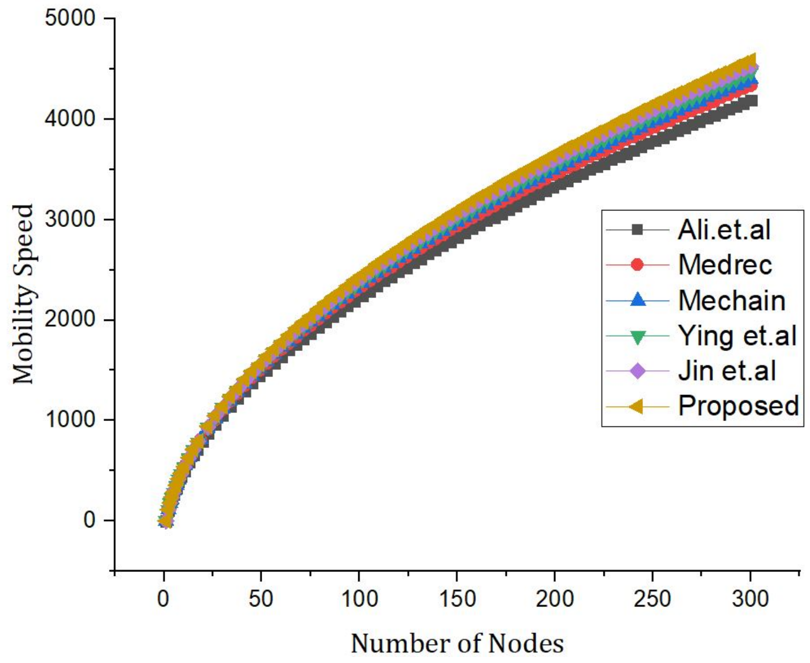

Figure 11. Comparative analysis of the proposed framework versus benchmark model based on the speed and number of nodes.

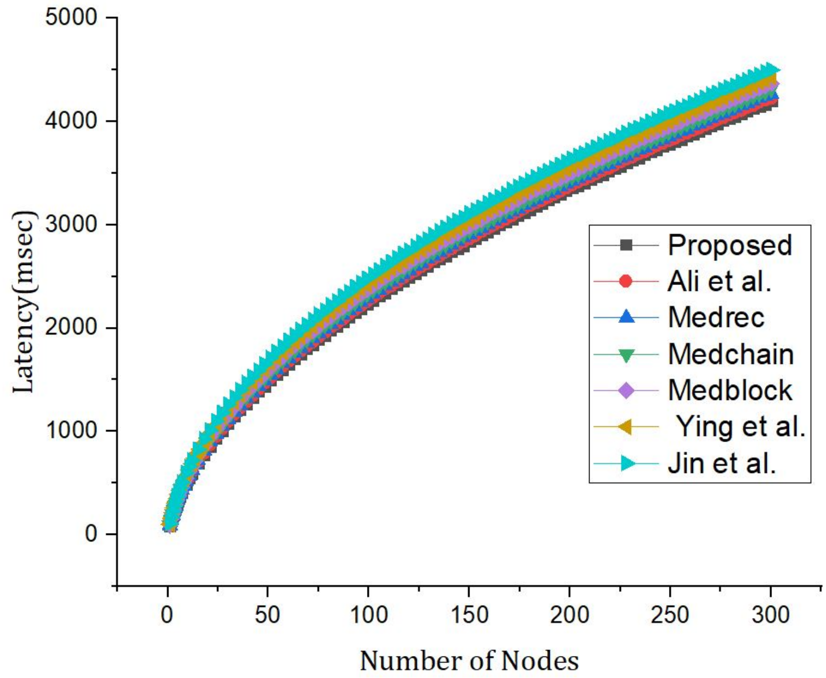

Figure 12. Comparative analysis with the proposed framework versus benchmark model based on the latency and number of nodes.

In Fig.11 the simulations results are based on number of rounds versus latency.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 May 2022 doi:10.20944/preprints202205.0220.v1

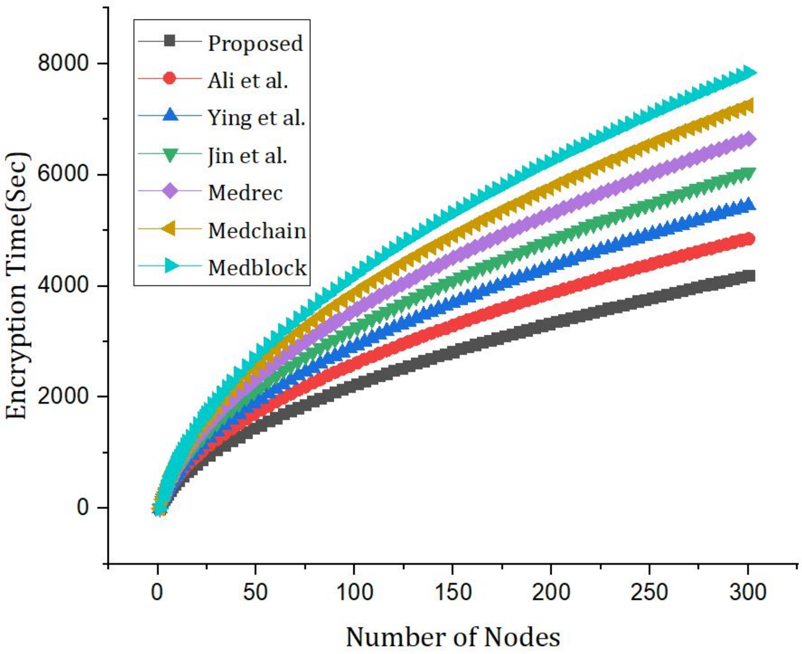

Figure 13. Comparative analysis based on number of nodes versus encryption time.

The comparative analysis based on the number of number of nodes and encryption time with the benchmark models. The proposed framework are compared with the the benchmark models which are mentioned on Fig.12. The text continues here. Proofs must be formatted as follows:

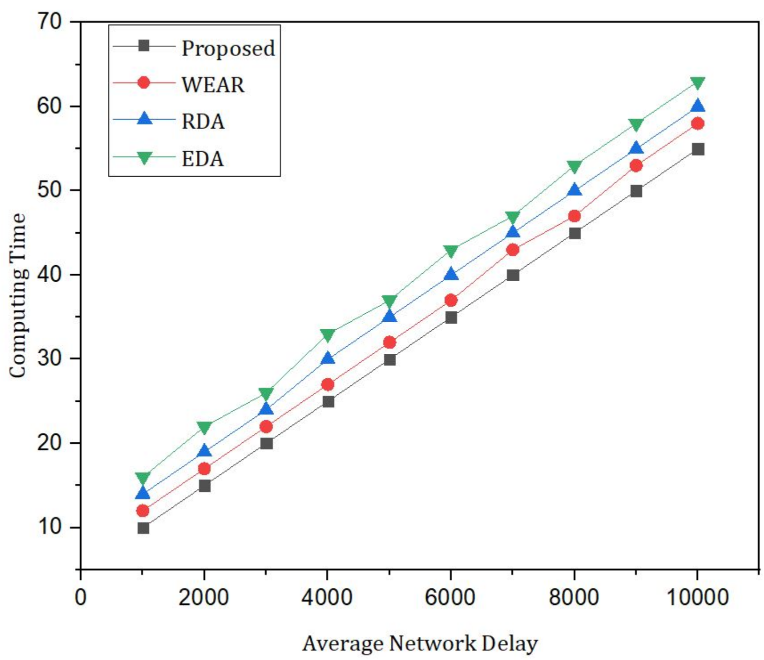

Figure 14. Comparative Analysis based on average network delay versus computing time.

Fig.13 reveal the simulations results based on number of average network delay versus computational time. The proposed protocol are compared with the WEAR, RDA and EDA protocol.

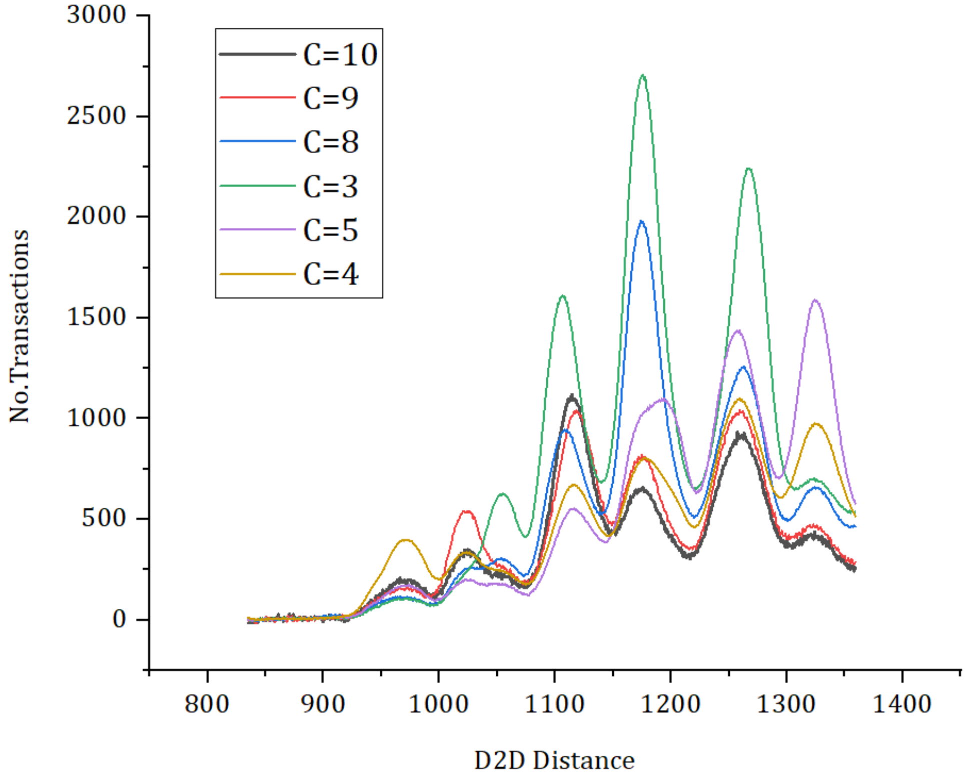

Figure 15. Comparative analysis based on d2d distance versus number of transactions.

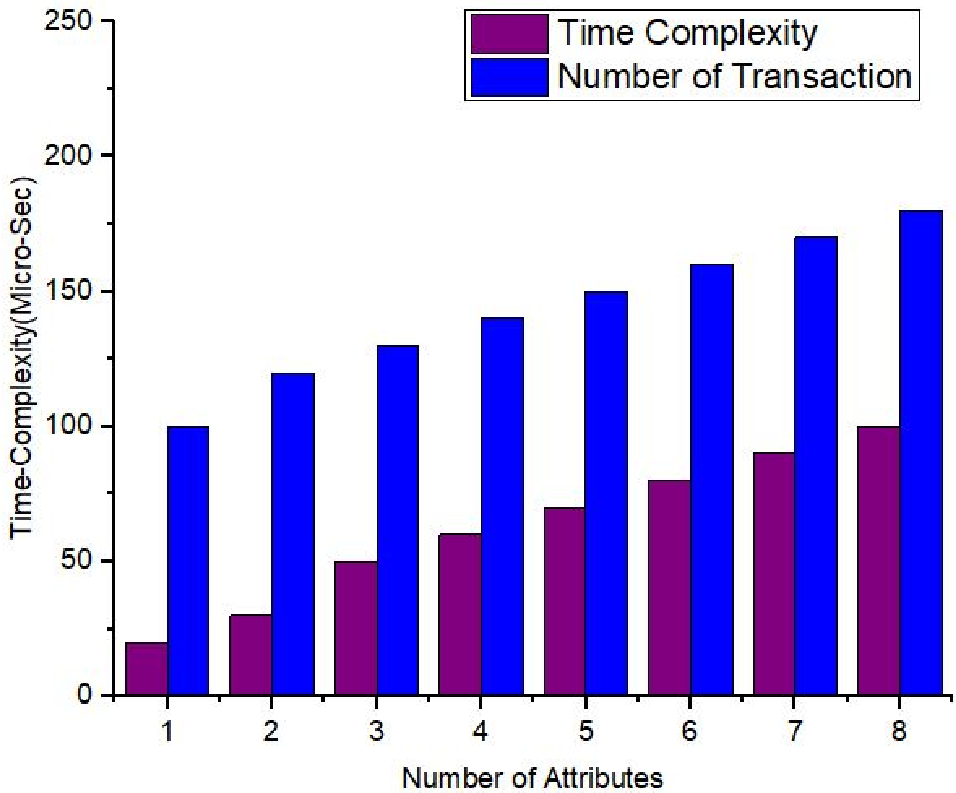

Figure 16. Comparative analysis based on d2d distance versus number of transactions.

In Fig.14 simulations results represent the comparative analysis of the proposed framework versus benchmark models. The comparison are based on no.transaction and d2d distance. Moreover, for the same number of distance between peer nodes the number of transactions varies. The proposed

7. Conclusions

This study analyses a privacy-preserving authentication system for industrial IoT applications. To reduce processing and communication expenses, TAB-SAPP uses hash evaluation and MAC verification. Massive IoT devices and cloud servers use service deniability to safeguard base-station access and user identities even when linked to open networks. It looked at the transaction's authenticated data blocks randomly. For example, TABSAPP's transmission rate is faster than existing TABSAPP due to faster calculation, connectivity, and mobility. As a result, the security and performance of computing, communication, and packet delivery can be improved.

References

1. A. A. Shah, G. Piro, L. A. Grieco, and G. Boggia, "A qualitative cross-comparison of emerging technologies for software-defined systems," in *2019 Sixth International Conference on Software Defined Systems (SDS)*, 2019, pp. 138–145.
2. A. Ali and M. Mehboob, "Comparative analysis of selected routing protocols for wlan based wireless sensor networks (wsns)," in *Proceedings of 2nd International Multi-Disciplinary Conference*, vol. 19, 2016, p. 20.
3. A. A. Shah, G. Piro, L. A. Grieco, and G. Boggia, "A review of forwarding strategies in transport software-defined networks," in *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, 2020, pp. 1–4.
4. R. R. Bruce, J. P. Cunard, and M. D. Director, *From telecommunications to electronic services: A global spectrum of definitions, boundary lines, and structures*. Butterworth-Heinemann, 2014.
5. V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: Is the technology mature enough?" *Future Internet*, vol. 10, no. 2, p. 20, 2018.
6. B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," *Sensors*, vol. 18, no. 11, p. 3894, 2018.
7. K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*. IEEE, 2016, pp. 1392–1393.
8. T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, and P. Fraga-Lamas, "Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and iot based continuous glucose monitoring system for diabetes mellitus research and care," *Sensors*, vol. 19, no. 15, p. 3319, 2019.
9. A. Ali, M. Naveed, M. Mehboob, H. Irshad, and P. Anwar, "An interference aware multi-channel mac protocol for wasn," in *2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT)*. IEEE, 2017, pp. 1–9.
10. A. Beebeejaun, "Vat on foreign digital services in mauritius; a comparative study with south africa," *International Journal of Law and Management*, 2020.
11. A. Aziz Shah, G. Piro, L. Alfredo Grieco, and G. Boggia, "A quantitative cross-comparison of container networking technologies for virtualized service infrastructures in local computing environments," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, p. e4234, 2021.
12. A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks," *IEEE Transactions on Network Science and Engineering*, 2019.
13. H. Kim, S.-H. Kim, J. Y. Hwang, and C. Seo, "Efficient privacy-preserving machine learning for blockchain network," *IEEE Access*, vol. 7, pp. 136 481–136 495, 2019.
14. A. Cirstea, F. M. Enescu, N. Bizon, C. Stirbu, and V. M. Ionescu, "Blockchain technology applied in health the study of blockchain application in the health system (ii)," in *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE, 2018, pp. 1–4.
15. A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE journal of biomedical and health informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.
16. V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health informatics journal*, vol. 25, no. 4, pp. 1398–1411, 2019.
17. Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.

18. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017, pp. 618–623.
19. L. Hang and D.-H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, 2019.
20. B. Yu, S. K. Kermanshahi, A. Sakzad, and S. Nepal, "Chameleon hash time-lock contract for privacy preserving payment channel networks," in *International Conference on Provable Security*. Springer, 2019, pp. 303–318.
21. K. Hameed, A. Ali, M. H. Naqvi, M. Jabbar, M. Junaid, and A. Haider, "Resource management in operating systems-a survey of scheduling algorithms," in *Int. Conf. on Innovative Computing (ICIC)*, vol. 1. University Of Management and Technology, 2016.
22. A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," *Sensors*, vol. 19, no. 2, p. 326, 2019.
23. E.-Y. Daraghmi, Y.-A. Daraghmi, and S.-M. Yuan, "Medchain: A design of blockchain-based system for medical records access and permissions management," *IEEE Access*, vol. 7, pp. 164 595–164 613, 2019.
24. Y. Jung, M. Peradilla, and R. Agulto, "Packet key-based end-to-end security management on a blockchain control plane," *Sensors*, vol. 19, no. 10, p. 2310, 2019.
25. C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.
26. C. W. Choo, *Information management for the intelligent organization: the art of scanning the environment*. Information Today, Inc., 2002.
27. S. K. Kermanshahi, J. K. Liu, R. Steinfeld, S. Nepal, S. Lai, R. Loh, and C. Zuo, "Multi-client cloud-based symmetric searchable encryption," *IEEE Transactions on Dependable and Secure Computing*, 2019.
28. S. K. Kermanshahi, J. K. Liu, and R. Steinfeld, "Multi-user cloud-based secure keyword search," in *Australasian Conference on Information Security and Privacy*. Springer, 2017, pp. 227–247.
29. S. K. Kermanshahi, J. K. Liu, R. Steinfeld, and S. Nepal, "Generic multi-keyword ranked search on encrypted cloud data," in *European Symposium on Research in Computer Security*. Springer, 2019, pp. 322–343.
30. Dwivedi.;, Ashutosh Dhar and Srivastava.;, Gautam and Dhar.;, Shalini and Singh.;, Rajani. A decentralized privacy-preserving healthcare blockchain for IoT Sensors, volume 19, number 2, pp.326,2019,Multidisciplinary Digital Publishing Institute
31. Rathi.;, Vipin Kumar and Chaudhary.;, Vinay and Rajput.;, Nikhil Kumar and Ahuja.;, Bhavya and Jaiswal.;, Amit Kumar and Gupta.;, Deepak and Elhoseny.;, Mohamed and Hammoudeh.;, Mohammad.; A blockchain-enabled multi domain edge computing orchestrator journal of IEEE Internet of Things Magazine, volume 3, number 2, pp. 30–36,2020, IEEE.
32. Nkenyereye.;, Lewis and Adhi Tama.;, Bayu and Shahzad.;, Muhammad K and Choi.;, Yoon-Ho.; Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing Sensors, volume 20, number 1, pp. 154,2020, Multidisciplinary Digital Publishing Institute.
33. eng.;, Chaosheng and Yu.;, Keping and Bashir.;, Ali Kashif and Al-Otaibi.;, Yasser D and Lu.;, Yang and Chen.;, Shengbo and Zhang.;, Di.; Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach IEEE Network, volume 35, number 1, pp.130–137,2021,IEEE.
34. Khujamatov.;, Khalimjon and Reypnazarov.;, Ernazar and Akhmedov.;, Nurshod and Khasanov.;, Doston.; Blockchain for 5G Healthcare architecture 2020 International Conference on Information Science and Communications Technologies (ICISCT), pp.1–5, 2020,IEEE.
35. Vivekanandan.;, Manojkumar.; and Sastry.;, VN and others.; BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology Peer-to-Peer Networking and Applications, volume 14, number 1, pp.403–419,2021,Springer.
36. Gao.;, Jianbin and Agyekum.;, Kwame Opuni-Boachie Obour and Sifah.;, Emmanuel Boateng and Acheampong.;, Kingsley Nketia and Xia.;, Qi and Du.;, Xiaojiang and Guizani.;, Mohsen and Xia.;, Hu.; A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks IEEE Internet of Things Journal, volume 7, number 5, pages 4278–4291,2019,IEEE.
37. Zhou, Sicong and Huang, Huawei and Chen, Wuhui and Zhou, Pan and Zheng, Zibin and Guo, Song pirate: A blockchain-based secure framework of distributed machine learning in 5g networks IEEE Network, volume 34, number 6, pp.84–91,2020,IEEE.
38. Zhang.;, Yan and Wang.;, Kun and Moustafa.;, Hassnaa and Wang.;, Stephen and Zhang.;, Ke.; Guest Editorial: Blockchain and AI for Beyond 5G Networks IEEE Network, volume 34, number 6, pp.22–23,2020,IEEE.
39. Yazdinejad.;, Abbas and Parizi.;, Reza M and Dehghantanha.;, Ali and Choo.;, Kim-Kwang Raymond.; Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks IEEE Transactions on Network Science and Engineering,2019,IEEE.
40. Zhao.;, Yang and Zhao.;, Jun and Zhai.;, Wenchao and Sun.;, Sumei and Niyato.;, Dusit and Lam.;, Kwok-Yan.; A survey of 6G wireless communications: Emerging technologies Future of Information and Communication Conference, pp. 150–170, 2021,Springer.
41. Bhattacharya.;, Pronaya and Tanwar.;, Sudeep and Shah.;, Rushabh and Ladha.;, Akhilesh.; Mobile edge computing-enabled blockchain framework—a survey Proceedings of ICRIC 2019, pp.797–809,2020,Springer.
42. Blockchain and 5G-Enabled Internet of Things: Background and Preliminaries Blockchain for 5G-Enabled IoT, pp.3–31,2021,Springer.

43. Mistry.;, Ishan and Tanwar.;, Sudeep and Tyagi.;, Sudhanshu and Kumar.;, Neeraj.; Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges Mechanical Systems and Signal Processing, volume 135, pp.106382,2020,Elsevier.
44. Budhiraja.;, Ishan and Tyagi.;, Sudhanshu and Tanwar.;, Sudeep and Kumar.;, Neeraj and Guizani.;, Mohsen.; CR-NOMA Based Interference Mitigation Scheme for 5G Femtocells Users 2018, volume 1, number 2, pp.1-6,10.1109/GLOCOM.2018.8647354.
45. Kermanshahi, Shabnam Kasra.; and Liu, Joseph K.; and Steinfeld, Ron.; Multi-user cloud-based secure keyword search Australasian Conference on Information Security and Privacy, pp.227–247, 2017,Springer.
46. Daraghmi, Eman-Yasser.; and Daraghmi, Yousef-Awwad.; and Yuan, Shyan-Ming.; MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management 2019, volume 7, pp.164595-164613,10.1109/ACCESS.2019.2952942,IEEE.
47. Wan, Zhiguo.; and Guan, Zhangshuang.; and Zhou, Yan.; and Ren, Kui.; zk-AuthFeed: How to Feed Authenticated Data into Smart Contract with Zero Knowledge 2019,pp.83-90,10.1109/Blockchain.2019.00020
48. in, Haiming.; and Su, Lu.; and Xiao, Houping.; and Nahrstedt, Klara.; Incentive Mechanism for Privacy-Aware Data Aggregation in Mobile Crowd Sensing Systems 2018, IEEE Press, vol.26, no. 5, issn 1063-6692,10.1109/TNET.2018.2840098.
49. Xiaoyi Pang.; and Dengfeng Guo.; and Zhibo Wang.; and Peng Sun.; and Liqiang Zhang.; Towards fair and efficient task allocation in blockchain-based crowdsourcing CCF Trans. Netw.,2020, vol.3, pp.193-204.
50. Ali, Aitizaz.; and Rahim, Hasliza A.; and Ali, Jehad.; and Pasha, Muhammad Fermi.; and Masud, Mehedi.; and Rehman, Ateeq Ur.; and Chen, Can.; and Baz, Mohammed.; A Novel Secure Blockchain Framework for Accessing Electronic Health Records Using Multiple Certificate Authority Applied Sciences, VOL.11,2021, No.21, ARTICLE-NUMBER.9999,https://www.mdpi.com/2076-3417/11/21/9999,2076-3417
51. Ali, Aitizaz.; and Rahim, Hasliza A.; and Pasha, Muhammad Fermi.; and Dowsley, Rafael.; and Masud, Mehedi.; and Ali, Jehad.; and Baz, Mohammed.; Security, Privacy, and Reliability in Digital Healthcare Systems Using Blockchain Electronics, VOL.10,2021, No.16, ARTICLE-No.2034,https://www.mdpi.com/2079-9292/10/16/2034,2079-9292.
52. Siam, Ali I.; and Almaiah, Mohammed Amin.; and Al-Zahrani, Ali.; and Elazm, Atef Abou.; and El Banby, Ghada M.; and El-Shafai, Walid.; and El-Samie, Fathi E Abd.; and El-Bahnasawy, Nirmeen A.; Secure Health Monitoring Communication Systems Based on IoT and Cloud Computing for Medical Emergency Applications Computational Intelligence and Neuroscience,2021,Hindawi.
53. Qasem, Mais Haj.; and Obeid, Nadim.; and Hudaib, Amjad.; and Almaiah, Mohammed Amin.; and Al-Zahrani, Ali.; and Al-Khasawneh, Ahmad.; Multi-Agent System Combined With Distributed Data Mining for Mutual Collaboration Classification IEEE Access, vol.9, pp.70531–70547,2021,IEEE
54. Almaiah, Mohammed Amin.; A New Scheme for Detecting Malicious Attacks in Wireless Sensor Networks Based on Blockchain Technology Artificial Intelligence and Blockchain for Future Cybersecurity Applications, pp.217,Springer
55. Almaiah, Mohammed Amin.;and Al-Zahrani, Mohammed.; Multilayer Neural Network based on MIMO and Channel Estimation for Impulsive Noise Environment in Mobile Wireless Networks International Journal of Advanced Trends in Computer Science and Engineering, vol.9, no.1, pp.315–321,2020