A Lightweight Identity-Based Signature Scheme for Mitigation of Content Poisoning Attack in Named Data Networking With Internet of Things

SYED SAJID ULLAH, INSAF ULLAH, HIZBULLAH KHATTAK, MUHAMMAD ASGHAR KHAN, MUHAMMAD ADNAN, SADDAM HUSSAIN, NOOR UL AMIN, AND MUAZZAM A. KHAN KHATTAK, (Senior Member, IEEE)

1Department of Information Technology, Hazara University Mansehra, Mansehra 21120, Pakistan
2HIEET, Hamdard University, Islamabad Campus, Islamabad 44000, Pakistan
3Higher Colleges of Technology, Al Ain, United Arab Emirates
4Department of Computer Science, Quaid-i-Azam University, Islamabad 44000, Pakistan
Corresponding author: Syed Sajid Ullah (sajidullah718@gmail.com)

ABSTRACT

Named Data Networking (NDN) is one of the future envisioned networking paradigm used to provide fast and efficient content dissemination with interest-based content retrieval, name-based routing and in-network content caching. On the one hand, this new breed of future Internet architecture is becoming a key technology for data dissemination in the IoT networks; on the other hand, NDN suffers from new challenges in terms of data security. Among them, a content poisoning attack is the most common data security challenge. The aim of this attack is to inject poisoned content with an invalid signature to the network. Therefore, to prevent NDN against possible content poisoning attack, a signature of the contents is appended to each data packet for verifications. In this paper, we propose an identity-based signature scheme for IoT-based NDN networks, with a special emphasis on content integrity and authenticity. The proposed scheme is based on the concept of the Hyperelliptic curves, which provide the same level of security as Rivest-Shamir-Adleman (RSA), Bilinear pairing and Elliptic Curve Cryptosystems (ECC) with lower-key size. The proposed scheme is subject to both formal and informal security analysis in order to show the feasibility of our scheme. Finally, the performance of the proposed scheme is analyzed via comparison with the relevant existing schemes that authenticates the superiority of our scheme in terms of security and efficiency.

INDEX TERMS

Content poisoning attack, named data networking (NDN), Internet of Things, identity-based signature.

I. INTRODUCTION

The Internet of Things (IoT) has been acknowledged as a potential deployment area for Named Data Networking (NDN) over the traditional host-to-host approach, due to the huge amount of data dissemination produced by the IoT devices [1]. The current host-to-host nature of the Internet is not suitable for handling these smart devices because of the issues such as high latency, less security, limited address spacing and caching, etc., and therefore may not be able to provide efficient content distribution to the end-users [2]. In order to cope up with these limitations, a new Internet paradigm, called Named Data Networking (NDN) is proposed [3].

NDN is equipped with the advanced features of in-network caching and name-based routing which provide better content accessing for end-users with efficient connectivity to IoT devices [4], [5]. Moreover, NDN deals with two types of packets i.e. interest packet and data packet. The interest packets are sent to retrieve a particular piece of data while the response to that particular interest is called data packet. The NDN node generally maintains three types of data structures, viz., Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB) [6]. The CS stores the data packets passing through the router that can be cached for future reuse. The PIT stores all the interests that a router has forwarded but not satisfied yet. The FIB is used to forward the interest packets from one router to another based on routing protocols [7].
Suppose a client A sends an interest for some contents as shown in the Figure 1. The particular interest of client A will be forwarded to the original content provider for the first time. However, the response in the form of data packets will be cached by the intermediate routers R4, R3, and R1 for future use. Later on, if client B requires the same piece of contents, the particular interest of client B will be satisfied locally from R3, instead of forwarding the interest to the original content provider. The in-network caching policy of NDN increases the response time of the overall network by providing the contents locally from its caches instead of forwarding the interest to the original provider [8]. In addition, NDN uses digital signature for signing every data packet for providing authentication and data integrity [9].

NDN faces some security issues in terms of the IoT network; one of the most common is the content poisoning attack [10]. The aim of this attack is to congest the cache with invalid contents that are normally signed with a fake signature [11]. In a content poisoning attack, the attacker takes full control of the intermediate router and send fake contents with an invalid signature to the client. Further, as NDN uses an in-network caching policy, therefore, the poisonous contents can be stored and forwarded in the entire network and hence can cause a massive disaster for the clients. A general scenario of content poisoning attack is shown in the Figure 2. In step 1, a client A shows an interest for some content. In step 2, after receiving the interest, the provider will provide the respective content with digital sign. According to NDN in-network caching policy, the intermediate routers between client A and provider, will keep the copy of the content in its CS for future reuse. Here, in the given scenario, the routers 3, 2, and 1 must store the copies of content in its CS and forwards the content to the client A. In step 3, an attacker takes control of the router 2 and forge the valid signature of the content by injecting a fake signature with poisonous content. In step 4, a client B, connected with router 5, shows an interest for the same content. In step 4, the router will act as a provider and will provide the poisonous copy of the content from its CS to the Client B and the intermediate routers 4, and 5 will store the poisonous copy of contents in its CS.

To prevent content poisoning attack, different solutions have been proposed in the literature [12]–[24]. Unfortunately, none of the solutions work effectively by providing a valid solution to the signature generation and verification. In digital signature, the private key of a particular signer is used to sign the content/message, while the public key is used for the authenticity of the signer [25]. However, it is a costly operation for every router, to verify the authenticity of each content with a Public Key Infrastructure (PKI) setting [26]. Therefore, IoT-based NDN network demands a lightweight signature scheme that can be used to solve the certificates management issues with minimal computation and communication costs.

Shamir in 1984 [27], proposed the first identity-based signature (IBS) scheme for solving the certificate related issues in PKI. The proposed work uses the identity of a signer for the calculation of the public key while the private key is generated by a third party named key generation center (KGC). Using the concept of Shamir, a number of schemes [28]–[32], [34], [35] and [36]–[53] have been proposed. However, none of the proposed solutions work effectively because of high incurring computation and communication costs. Further, the proposed schemes are mainly based on bilinear pairing and elliptic curves that perform heavy computational operations which are not a suitable option for resource-constrained IoT devices. Moreover, these schemes are not validated through any sort of formal security validation tools such as Automated Validation of Internet Security Protocols and Applications (AVISPA) or Scyther etc. that can, somehow, guarantee security.

A. AUTHOR’S MOTIVATIONS AND CONTRIBUTIONS

Motivated by the above, in this paper, we propose an identity-based signature scheme for the prevention of content poisoning attack in the IoT-based NDN networks. The proposed scheme is based on the advanced version of elliptic curves, called the Hyperelliptic curve [54]. The Hyperelliptic curve provides the same level of security as Rivest-Shamir-Adleman (RSA), Bilinear pairing and Elliptic Curve Cryptosystems (ECC) with smaller key size [55]. Moreover, our scheme prevents content poisoning attack with less verification overhead and keeps the caches clean from invalid contents. Furthermore, the client can authenticate the provider’s and verify the integrity of the content in order...
to reduce verification overhead. To achieve this, we studied different ID-based signature [36]–[53] schemes that are designed for IP-based Internet architecture. The aforementioned schemes lead us to show some contributions which are as follows:

- We propose an efficient and formally secure identity-based signature scheme for preventing content poisoning attack in IoT-based NDN environment.
- We use a lightweight Hyperelliptic curve algorithm for the efficiency in terms of computational and communication costs.
- For formal security analysis, we validate our scheme through a well-known validation tool, i.e., Automated Validation of Internet Security Protocols and Applications (AVISPA).
- We also provide provable security through random oracle model (ROML) regarding existential unforgeability against adaptive chosen content (message) attack (EUF – IBS – ACCA).
- We compare our scheme with existing content poisoning attack schemes and the theoretical discussion shows that our scheme prevents content poisoning attack with low latency and less verification overhead.
- We also compare our scheme with existing ID-based signature scheme, the final results show that our scheme is much more efficient and highly secured from its existing counterparts.
- We also provide a practical implementation of our proposed scheme in the application scenario of NDN-based smart city.

**B. PAPER ORGANIZATION**

In Section II, we discuss the related work about content poisoning attack in NDN and Identity-based Signature schemes. Section III describes the preliminaries for our proposed scheme. Section IV discusses the proposed mechanism and its algorithms. In section V, we discuss and compare the proposed scheme with existing schemes. In section VI, we described the application scenario and practical deployment for the proposed scheme. Section VII provides conclusions. Section VIII contains the appendix of the simulation code and results.

**II. RELATED WORK**

Researchers have presented different solutions for mitigation of content poisoning attack in recent times. However, they are struggling to protect NDN from this prominent attack. Here, we divide the related work into two parts; NDN based solution for content poisoning attack and Identity-based Signature schemes.

**A. CONTENT POISONING ATTACK PREVENTION SCHEMES IN NDN**

In 2013, Gasti et al. [10] proposed probabilistic signature verification using the “self-certifying interest/data packet” (SCID) for helping the routers to authenticate every receiving chunk of the content. However, due to the extra overhead on the router, the proposed approach failed to perform well. Ghali et al. [12] added interest-Key Binding (IKB) to the interest packet in order to bind the content name and provider public key. A key locator puts the provider key to the interest. However, signature and PKI based verifications are a slow process and cannot be able to perform at line speed. Ghali et al. [13] further proposed a ranking algorithm for reducing the overhead of routers. The aim of this algorithm is to differentiate between valid and invalid content on the basis of observed consumer behavior. It prioritizes valid content over invalid in reply to consumer interests. However, it verifies each content that creates overhead and it also rejects a valid content due to abnormal behavior of valid content and stores the invalid content.

Kim et al. [14] proposed a check before storing (CBS) mechanism for reducing the cost of the signature verification. This mechanism probabilistically checks and verifies content items and only stores the validated content items in CS. It divides content into two types, cache hit, and cache miss. In case of a cache hit, it stores the content and in the latter case, bypass it. For cache replacement, it uses a segmented Least Recently Used (LRU) policy in which content is initially placed in the unprotected section of the cache and then upon successful verification, it is moved to the protected one. It just verifies the signature of a serving content that has a first cache hit. The limitation of this scheme is the latency that occurs due to the verification process for every chunk that is requested twice. Hence, an attacker can enforce verification of each invalid content by requesting it twice. A valid content can be bypassed and fake content can be stored through this mechanism. Kim et al. [15] further looked at its own work [9], particularly the verification attack and proposed scheme to exploit the relationship between the number of serving content and the amount of cache-hit events to defend against verification attack. Nguyen et al. [16] experimentally measured content poisoning attack and concluded that it can easily and badly affect NDN.

Baugher et al. [17] presented self-verifying names for the shifting authentication mode of ICN. It ensures the authenticity of data for read-only named data. The limitation of this scheme is that invalid users can sign fake data from the providers. Bianchi et al. [18] and Detti et al. [19] presented ‘Lossy Caching’. In Lossy Caching, content is authenticated and stored with a certain probability. But the probability affects the hit ratio and the recency of network caches. The problem is to find out the best possible probability value. The scheme is not compatible with different cache replacement policies. Dibenedetto and Papadopoulos et al. [20] presented on-path content poisoning detection and avoiding mechanism. In this scheme, consumers have to send some additional information to routers. The routers maintain a naming list of coming data packets with their interfaces and aggressively send traffic to look at other valid paths. We argue that these places are creating additional overhead on both users and routers.
Wu et al. [21] presented Router-Oriented Mitigation (ROM) scheme which offers security assurance even when the caches are injected. ROM temporarily removes injected routers from the transmission, introduces reputation for every router and forwards content on the basis of these reputations. However, sometimes a valid router acts like an injected one; if there is no alternative path for the transmutation. Mai et al. [22] proposed a Bayesian Network techniques approach for examining and discovering irregularity in NDN routers. They introduced a record of checked metrics as a numerical measure to mark the behavior of the router. They developed a micro detector for checking and detecting normal to abnormal behavior. The proposed network structure associates alarms from micro detectors and its design are based on the expert knowledge of NDN specification and NFD implementation. The performance and significance of the Bayesian Network techniques approach confirm that this attack is very alarming in NDN. Long Mai et al. [23] further used the Montimage Monitoring Tool (MMT) for the detection of content poisoning attacks in which the orchestrators can respond for the alleviation of its impact on the network. The authors only experimented with the effect of a content poisoning attack, but they do not provide any solution for avoiding this attack. It is a very costly process to pass each content from the micro detector.

Hu et al. [24] proposed a light-weight mitigation mechanism; name-key-based forwarding and multipath forwarding-based inband probe. In the first one, the interest is forwarded toward trusted content sources in order to decrease the insertion of poisoned content. If poisoned content is still there on the on-path, the multipath forwarding of a reissued interest that rejects poisoned content acts as inband probes and perform on-demand signature verification at the middle routers. This removes invalid content from routers and sends valid content to the present user. It also restores valid content recovery for future interests with no need for any out-of-band communications. After the request, a client should obtain the key of the provider. The limitation is if there is no matching key for the interest in FIB the interest will be discarded. Divergent has many disadvantages like collision may occur by all traffic on one side, it also leads to a denial of service attack. Interest can be forwarded, where no source is available for data.

B. IDENTITY-BASED SIGNATURE SCHEMES

In 1984, Shamir [27] introduced the concept of identity-based signature to solve the certificate management issues of public-key cryptography (PKC). Later on, many ID-based signature schemes were introduced [35]–[37] by using the concept of Shamir [27]. In 2001, Sahu and Padhye [37] introduced a full workable ID-based encryption (IBE) scheme by using bilinear pairs. This idea leads Boneh and Franklin et al. [38] to propose the ID-based signature scheme (IBS) over bilinear pairings. In 2003, Cha and Cheon [40] proposed an ID-based signature scheme using Gap Diffie–Hellman. The scheme ensures unforgeable protection against ID-based attacks in the random oracle model. In the same year later, Hess [41] proposed an ID-based signature scheme that provides security based on the computational Diffie–Hellman Problem (DHP) by using the random oracle model.

In 2005 Xu et al. [42] proposed an ID-based signature scheme for authentication in Mobile Ad Hoc Network. This scheme worked on offline/online concepts and provide security against forged-ability attacks. The aim of the offline/online concept to divide the signature into two steps, offline step and online step. In the offline step, the signature is performed without knowing the message. The online step allows the signer to know the message before signing. Further, in 2006, Xu et al. [43] proposed an ID-based signature scheme to improve [42] for multi-signature support. In 2007, Du and Wen [29] proposed a short ID-based signature scheme to reduce signature computation cost. In 2008, Li et al. [44] proved that the security of [43] scheme is weak and easily breakable. In 2009, Zhang et al. [45] proposed an IBS scheme using the random oracle model to improve the weakness of [43]. In 2010, Liu [46] proposed an authentication scheme for wireless sensor networks to use offline storage multiple times in polynomial time. The silent feature of this scheme is that there is no need for a pairing operation. Further, in 2012 Li et al. [47] proposed the PF-IBS algorithm to reduce the computation cost. In 2014, Le and Fang [48] proposed an ID-based signature for message recovery. The authors used the random oracle model for security proof based on the Bilinear Diffie-Hellman model. The scheme is improved in 2015, by Chen et al. [49] by proposing an ID-based blind signature to protect user identity and validate signer. In 2016, Z. Qin et al. [50] proved the security of some schemes and point out that these schemes suffer from forgery attack and security can be easily compromised. In 2017, Sharma et al. [51], proposed a pairing-free IBS scheme in the random oracle model. The aim of this scheme is to reduce signature computation cost and safety from forging signature attacks. For checking the performance of this scheme, the authors used MICAz with TinyOS and RELIC-Toolkit. In 2018, Sharma and Sharma [34] proposed an IBS scheme using the bilinear map in the random oracle model to reduce the communication cost and provide a more secure signature. The authors proved the security of the proposed scheme under the computational Diffie-Hellman problem. In the same year, James et al. [52] proposed an IBS scheme for signature and message recovery. In the proposed scheme, the authors used bilinear pairings over Elliptic Curves to reduce signature cost. Additionally, they also proved the correctness and security of this scheme.

In 2019, Krishna et al. [53] proposed an IDS scheme without using pairings over the elliptic curve to reduce the computation and communication costs. The authors proved the security of the scheme under the elliptic curve discrete logarithm problem (ECDLP). Recently, Yaduvanshi and Mishra [35] proposed a short IBS scheme over the elliptic curve without using bilinear pairing to reduce
computation cost. Further, the scheme is proved under the assumption of the ECDL problem.

The schemes [34], [35], [42]–[53] in the literature, suffer from high computational and communicational requirements which is not a suitable choice for the resource-constrained IoT devices.

Moreover, the aforementioned schemes are specially designed for the IP-based architecture of the Internet. To make it capable for IoT-based NDN network and for the prevention of content poisoning attack, a lightweight signature scheme is required, which can provide strong security with less computation and communication resources.

III. PRELIMINARIES

A. HYPERELLIPTIC CURVE

At first, we discuss shortly the Hyperelliptic curve $(\mathcal{H})$. Let $\mathcal{g}$ be a finite set and assume $\mathcal{d}$ is the genus of $\mathcal{H}$ with an order of $\mathcal{d} \geq 2$. Suppose $(\mathcal{V})$, $f(\mathcal{V}) \in \mathcal{g}[\mathcal{V}]$, and deg $(f(\mathcal{V})) \leq \mathcal{d}$; further $f(\mathcal{V})$ is a monic polynomial having deg $(f(\mathcal{V})) = 2\mathcal{d} + 1$ [56]. Moreover, $\mathcal{H}$ of genus $\mathcal{d} \geq 2$ over $\mathcal{g}$ is a set of points $(\mathcal{V})$, $\mathcal{g}^*\mathcal{g}$ as mentioned in the equation (1).

$$\mathcal{f} : \hat{w}^2 + (\mathcal{V})\hat{w} = f(\mathcal{V})$$  

(1)

Note that $\mathcal{f}$ points are totally different from the elliptic curve [57]. In case of the divisors that are the formal sum of the finite integer such as $\mathcal{d} = \sum x_i z_i$ where $x_i \in \mathcal{g}$ and $z_i \in \mathcal{H}$ $\mathcal{f} \mathcal{H}$. Moreover, in case it forms Jacobian group $\mathcal{J}$ having the following brief order.

$$(\mathcal{V}_{\mathcal{T}-1})^{2\mathcal{d}} \leq \mathcal{H}_{\mathcal{f} \mathcal{H}}(\mathcal{g}) \leq (\mathcal{V}_{\mathcal{T}+1})^{2\mathcal{d}}$$  

(2)

1) HYPERELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM

Suppose $\mathcal{d}$ is a divisor which is known to everyone publicly in the entire network and $\mathcal{L}$ is picked as a random private number from $\mathcal{g}$, then recovering $\mathcal{L}$ from $\mathcal{d} \mathcal{L}$ is known to be $\mathcal{f} \mathcal{H} \mathcal{d} \mathcal{L}$ discrete logarithm problem.

B. SYNTAX OF IDENTITY-BASED SIGNATURE

The proposed identity-based signature scheme is the extended version of [35], which consists of the four algorithms: setup, key generation, Provider-Signature Generation, and Client-Signature Verification, respectively. The basic syntax of the proposed scheme is discussed in the following mentioned steps.

- In this algorithm, given $\phi$ as a security parameter, the network manager picks a secret key as $\mathcal{V}$ and processed a public key $\mathcal{V}$. Generates all public parameters set $\mathcal{V}$ and publishes it.

- **Key Generation**: The network manager takes the identity of each user $\mathcal{I} d_u$ as an input and generates the private key $\mathcal{Q}_u$ and public key $\mathcal{w}_u$ for the $\mathcal{I} d_u$.

- **Provider-Signature Generation**: This algorithm is run by the provider and it takes the divisor $D$, private key $\mathcal{Q}_u$ and content $\mathcal{C}$ as an input and generate sign tuple $\delta$.

- **Client- Signature Verification**: This algorithm is normally executed on the client-side in which the client calculates the public key $\mathcal{w}_p$ and the hash function $\mathcal{W}$ to verify $\delta$.

C. THREAT MODAL

In the proposed scheme, for the transmission of content among producer and client, we consider the Dolev-Yao (DY) [55], [55], model. According to DY, the communication between two parties is performed in an open channel. In the DY threat model, the attacker has a full command to modify the content, forge the signature in any IoT-based NDN network. Further, the IoT-based NDN network has the ability to detect the behavior of the malicious user inside the network. To modify the content and forge the signature, the attacker tries to launch a content poisoning attack. To maintain the security and prevent content poisoning attack in the IoT-based NDN network it is really important to validate all users from its signature.

The identity based signature scheme is considered to be existential unforgeability against adaptive chosen content (message) attack (EUF – IBS – ACCA). If there is no intruder ($\mathcal{JNT}$) with the polynomial bonding running time, while inputting the common parameters ($\mathcal{Param} = \mathcal{\bot}$), wins the following game with a non-negligible probability. The challenger $\mathcal{J}$ commanding the game and will have to be responded to the $\mathcal{JNT}$ queries.

1. The $\mathcal{JNT}$ issues key generating queries $\mathcal{Q}_{\mathcal{KG}}$, for the given identity $\mathcal{I} d_u$, for this purpose the challenger $\mathcal{J}$ will run the key generating query by providing the input identity $\mathcal{I} d_u$, further, obtain the corresponding private key $\mathcal{Q}_u$ and provide it to the $\mathcal{JNT}$.

2. The $\mathcal{JNT}$ issue the Provider-Signature Generation Queries $\mathcal{Q}_{\mathcal{PSG}}$ as an input, further, obtain the corresponding private key $\mathcal{Q}_u$. After that, $\mathcal{J}$ run the Provider-Signature Generation algorithm by providing the $\mathcal{Q}_u$ as an input and provide it to the $\mathcal{JNT}$ with the resultant signature $\delta$.

3. The adversary $\mathcal{JNT}$ generate $(\delta')$ by taking $\mathcal{I} d'_u$ and $\mathcal{C}'$ as an input. The $\mathcal{Q}_{\mathcal{KG}}$ and $\mathcal{Q}_{\mathcal{PSG}}$ never have been called for $\mathcal{I} d'_u$ and $\mathcal{C}'$ before.

The $\mathcal{JNT}$ take message $\mathcal{C}'$ and $\mathcal{\bot}$ as an input and generate $\delta'$ as a signature. The probability of the adversary winning the game is decided from the advantage of the $\mathcal{JNT}$. The $\mathcal{JNT}$ is declared to be the $(u, \tau, \mathcal{Q}_{\mathcal{KG}} \mathcal{Q}_{\mathcal{PSG}} \mathcal{Q}_u)$ forger, if it has at least advantages in the aforementioned game. The $\mathcal{JNT}$ may run for at most $(\tau)$ time, while making at most $\mathcal{Q}_{\mathcal{KG}}$ extraction queries, $\mathcal{Q}_u$ hash queries with $\mathcal{Q}_{\mathcal{PSG}}$, sign queries in the random oracle model (ROM). The algorithm is considered to be secure against the (UF – IBS – ACCA) if there exist no $(u, \tau, \mathcal{Q}_{\mathcal{KG}} \mathcal{Q}_{\mathcal{PSG}} \mathcal{Q}_u)$ forger. The abbreviation used in preliminaries and algorithm sections is mentioned in Table 1.

IV. PROPOSED SCHEME

Here, we proposed a lightweight OnDemand verification authentication scheme for mitigating content poisoning attacks in IoT-based NDN network. In our scheme all the providers and the clients register themselves with the network manager by providing their identities, then the network manager generates public and private keys by using their
identities. Whenever the client shows an interest for some contents, the NDN routers forward that particular interest towards the provider as indicated in Figure 3. Upon receiving the interest the provider applies Hash on the requested content to get the message digest ($MD_1$) and digitally signs the $MD_1$ with his private key. After that, the requested content is delivered to the client with the digital signature and $MD_1$ of the provider. The requested content is stored in caches of R-1, R-2, and R-4 by following leave copy everywhere (LCE) caching policy as shown in Figure 1.

Suppose, an attacker poisoned the original content A in R-2 as shown in Figure 4. Later, if another client B shows interest for the same contents A and that interest is received at R-2, here, the R-2 will send the poisoned copy to client B as shown in Figure 5 (step-4).

Here, if client B wishes to verify the received contents A due to its importance, it sends a request to NA for the corresponding public key of the original content provider. After receiving the public key, the client B tries to verify the digital signature with the corresponding public key of the provider. If it decrypts with the public key, then it means the publisher is registered with the NA and is an authentic provider. In this way, the original provider is authenticated.

After the authentication phase, if client B wants to check the integrity of the content. It simply applies Hash on the received content to get the message digest $MD_2$. The Client B than compares the computed $MD_2$ with the received $MD_1$. If both message digests are equal, it means the content has not been poisoned otherwise the content has been poisoned. If the content is poisoned, then the client B encrypts the poisoned contents A and $MD_2$ with the public key of the valid provider and sends it to the original provider. After receiving, the provider decrypts $MD_2$ with its private key and compares it with its valid content $MD_1$. At the end, original provider broadcasts a message regarding this poisoned content in the networks to remove it from the router caches.

**A. PROPOSED SCHEME ALGORITHMS**

This phase contains a brief discussion of the proposed scheme and its algorithms. The abbreviations used in our proposed algorithm are shown in Table 2. The scheme consists of three participants, namely; the network manager, provider of contents and the client.

| Table 2. Comparison and discussion. |
|-------------------------------------|
| Authors                             | Scheme                  | Latency | Verification Overhead | Security Level |
| Ghali et al. [13]                   | Ranking Algorithm       | Low     | Overhead              | Weak           |
| Kim et al. [15]                     | Security of Cached      | High    | Extra                 | Average        |
| D. Wu et al. [21]                   | Content in NDN          | High    | Extra                 | Weak           |
| H. L. Mai et al. [22]               | Mitigation (ROM)        | High    | Less                  | Average        |
| X. HU et al. [24]                   | Towards a Security      | High    | Overhead              | Average        |
|                                    | Monitoring Plane for    |         |                       |                |
|                                    | NDN                     |         |                       |                |
| Proposed                            | Mitigating Content      | High    | Less                  | Average        |
| Scheme                              | Poisoning with          |         | Overhead              |                |
|                                    | Name-Key Based Forwards |         |                       |                |

The proposed scheme consists of four algorithms [51]: setup, key generation, provider and client verification. We processed our proposed scheme algorithm in the following step:

**Setup:** In this algorithm, given $\phi$ as a security parameter, the network manager picks a secret key as $\forall \in \{1, 2, 3, \ldots, q-1\}$ processed a public key as $\Gamma = \forall.D$, where $D$ is the divisor of the hyperelliptic curve ($f(x)$). Generates all public parameters as $\forall := (h_0, h_1, \Gamma, f(x), g, d, \phi, J, D)$ and publishes it, where $(h_0h_1)$ are the one way collision resistant hash functions.

**Key Generation:** This algorithm enables a network manager to generate a public and private key for a user with the identity $Id_u$ by using the followed computations.
1) The network manager first randomly chooses $v_u \in \{1, 2, 3, \ldots, q-1\}$ and computes $w_u = v_u \cdot D$.
2) Compute $\overline{c} = h_0(3d_uw_u)$ and $\beta = \overline{c} \cdot \Gamma$
3) Compute $\Omega_u = (v_u + \overline{c} \cdot \nabla) \mod q$
4) Set $\Omega_u$ is the private key for the user with the identity $3d_u$
5) Set $w_u$ is the public key for the user with the identity $I_d_u$
6) Give $(\Omega_p w_u)$ to the user with the identity $I_d_u$ through secure network

**Provider-Signature Generation:** This algorithm is executed by the provider. It takes the Divisor $D$, the private key of the provider $p$ and the content $C$ as an input to produce a sign tuple $\delta = (C, W, L, S)$.

1) A provider first Randomly chooses $d \in \{1, 2, 3, \ldots, q - 1\}$
2) Computes $L = d, D \ mod \ q$
3) Computes content digest $W = h_1(C // L // N_r // I_d_p)$, where $N_r$ is the fresh nonce
4) Set $W = MD_1$
5) Computes $S = (\Omega_p W + d) \ mod \ q$
6) Sends a sign tuple $\delta = (C, W = MD_1, L, S)$ to the client

**Client-Signature Verification:** Upon receiving $\delta = (C, W, L, S)$, the client can verify the contents in the following steps:
- Computes content digest $W = h_1(C // L // N_r // I_d_p)$
- Set $W = MD_2$
- Computes $S.D = W (w_p + \beta) + L$ for signature verification
- Compare $MD_2 = MD_1$ for integrity, if it is not holds, then it means that the content is poisoned.

**Poisoned Content Removing:** Once the content is poisoned, then client B and provider perform the followed steps.
- The client B encrypts the poisoned contents $A$ and $MD_2$ as $POJ = E_{w_p} (A, MD_2)$
- Sends $POJ$ to the original publisher
- After receiving $POJ$, the publisher decrypts $(A, MD_2) = D_{\Omega_p}(POJ)$
- Compares $MD_2$ with its valid content $MD_1$ as $MD_2 = MD_1$. If the equality does not hold, then original publisher broadcasts a message regarding this poisoned content in the networks to remove it from the router caches

**B. CORRECTNESS**
If the client wants to verify the received contents, then it performs the following computation:

$$S.D = W. (w_p + \beta) + L$$
$$S.D = (\Omega_p W + d) \cdot D = (\Omega_p W + d) \cdot D$$
$$= (\Omega_p W, D + d, D) = (W, D (w_p + \varepsilon, V) + d, D)$$
$$= (W, (w_p, W + \varepsilon, V, W) + d, D)$$
$$= (W, (w_p + \beta) + L)$$
C. SECURITY ANALYSIS

1) UNFORGEABILITY (EUF – IBS – ACCA)

The proposed scheme can be secured against existential unforgeability against adaptive chosen content (message) attack (EUF – IBS – ACCA), if the intruder (\(\mathcal{JNT}\)) has the non-negligible advantage \(\xi\), and \(\mathcal{JNT}\) can request most of the time \(\tau\) for the queries such that, hash queries \(Q_h\), key generating queries \(Q_K\), and Provider-Signature Generation queries \(Q_{PSG}\) with \(\xi \geq (10(Q_{h0} + 1)Q_{h0} + Q_{PSG})/2^\phi\), then the challenger \(\mathcal{S}\) with executing time \(\tau' \leq (23Q_{h0}^\phi)/\xi\) and probability \(\xi' \geq 1/9\) [51], [54], can solve HECGLP.

**Proof:** let \(\gamma = \nabla.D\), where \(\nabla \in \{1, 2, 3, \ldots, q - 1\}\) so it is the task of \(\mathcal{S}\) to extract \(\gamma\) from \(\gamma\), which is called HECGLP. Then, \(\mathcal{S}\) sets the public parameters as \(\underline{\underline{\Delta}} = (h_0, h_1, \Gamma, \xi, \epsilon, s, c, \phi, J, D)\), where \((h_0, h_1)\) are the one-way collision-resistant hash functions. \(\mathcal{S}\) can answer the submitted queries of \(\mathcal{JNT}\) with the following steps.

**h0 queries:** when \(\mathcal{JNT}\) ask for \(h_0\) queries with tuple \((3d_wu)\), then \(\mathcal{S}\) search a variable \(n_1\) in \(h_0^{list}\), if such triple \((3d_wu, n_1)\) exists, \(\mathcal{S}\) outputs \(n_1\) otherwise, it randomly selects \(n_1 \in \{1, 2, 3, \ldots, q - 1\}\) and returns \(n_1\).

**h1 queries:** when \(\mathcal{JNT}\) ask for \(h_1\) queries with \((C/\ell/νu/I_du)\), then \(\mathcal{S}\) search a variable \(n_2\) in \(h_1^{list}\), if such triple \((3d_wu, n_2)\) exists, \(\mathcal{S}\) outputs \(n_2\) otherwise, it randomly selects \(n_2 \in \{1, 2, 3, \ldots, q - 1\}\) and returns \(n_2\).

**Key Generating Queries \(Q_{KG}\):** When \(\mathcal{JNT}\) submits a request with \(3d_w\), then \(\mathcal{S}\) randomly selects \(x, y \in \{1, 2, 3, \ldots, q - 1\}\), sets \(w_u = \chi, \gamma + y.D, u = y, \epsilon = h_0(3d_wu) = –x \mod q\), and \(\beta = \Gamma.D\). So, \(\mathcal{S}\) returns the tuple \((3d_wu, Q_{h0}(3d_wu))\) to the list \(h_0^{list}\).

**Provider-Signature Generation Queries \(Q_{PSG}\):** When \(\mathcal{JNT}\) submits a request with \(3d_w\), then \(\mathcal{S}\) can perform the below steps:

1. Check the \(3d_w\), if it is already submitted for hash queries \(Q_h\) or key generating queries \(Q_{KG}\), it returns \((3d_wu, Q_{h0}(3d_wu))\) from the list \(h_0^{list}\) to perform the Provider-Signature Generation process as like of section (A). Here, \(\mathcal{S}\) produced \(\delta\) and inserts \(h_1(C/\ell/νu/I_du)\) into \(h_1^{list}\).

2. If it is not being submitted for key generating queries \(Q_{KG}\), then \(\mathcal{S}\) processed this oracle, get the private key, and make a signature.

3. Otherwise, \(\mathcal{S}\) randomly selects \(x, y \in \{1, 2, 3, \ldots, q - 1\}\), calculate \(\mathcal{L} = \chi.D = y.w_u – y.\epsilon.\Gamma\), where \(\epsilon = h_0(3d_wu)\) is obtained from the list \(h_0^{list}\), sets \(\chi = \mathcal{S}\), and \(y = W\). Then, it inserts \((C/\ell/νu/I_du)\) into \(h_1^{list}\). Here, it should be noticed that if \((C/\ell/νu/I_du)\) exists in \(h_1^{list}\), then \(\mathcal{S}\) response is a flop and exists. So, \(y\) is a uniformly selected number, here, the probability failure is none extra then \(1/2\), which can be ignored.

When \(\mathcal{JNT}\) has the capacity derived the same signature such that Provider-Signature Generation process as like of section (A), for \(C\) with \(\xi \geq (10(Q_{h0} + 1)Q_{h0} + Q_{PSG})/2^\phi\). Here, it is to be noted that when \(\mathcal{C}\) has not been submitted to the Provider-Signature Generation oracle, then \(\mathcal{S}\) can make two valid signatures that are \(\delta = (\mathcal{C}, W, \mathcal{L}, s)\) and \(\delta' = (\mathcal{C}, W', \mathcal{L}, s')\). So, we have the following verification processes:

Firstly,

\[
S.D = (\Omega_wW + d).D = (\Omega_wW + d).
\]

Secondly,

\[
S'.D = (\Omega_wW + d).D = (\Omega_wW + d).
\]

Suppose \(L = d.D, w_u = x.\Gamma + y.D, \) and \(\gamma = \nabla.D = \Gamma,\) then we have the equalities like followed.

\[
S.D = (((W.x.\Gamma + W.y.D) + \epsilon.\nabla.D.W.D) + d.D)
\]

And,

\[
S'.D = (((W'.x.\Gamma + W'.y.D) + \epsilon.\nabla.D.W.D) + d.D)
\]

Then, \(S'S.D = (S'.d.D + S'.W.x.\nabla.D + W'.y.D + \epsilon.\nabla.D.W.D)\) and \(S'S.D = (S'.d.D + S'.W.x.\nabla.D + W'.y.D + \epsilon.\nabla.D.W.D)\).

So, if we perform the subtraction, then we have \((S.d - S'.d + S'.W.y - S'.W.y).D = (S.W'.x - S'.W.x + S.W'.W - S'.W.W).\nabla.D)\).

Then, \((S.d - S'.d + S.W.y - S'.W.y) = (S.W'.x - S'.W.x + S.W'.W - S'.W.W).\nabla.D)\). Then we have \(\nabla = (S.d - S'.d + S.W.y - S'.W.y) - (S.W'.x - S'.W.x + S.W'.W - S'.W.W).\nabla.D)\).

D. MITIGATION OF CONTENT POISONING ATTACK

In our proposed scheme, the producer generates a hash value \(W\) and digital signature \(S = (\Omega_pW + d)\mod q\) of a content \(C\). After that, the producer sends a tuple \(\delta = (\mathcal{C}, W, \mathcal{L}, s)\) to the client through an open network. Upon receiving \(\delta\), the client verifies the digital signature; check if \(S.D = W(w_u + \beta) + L\) which is already proven in section (B). Otherwise, invalid contents are broadcasted to the routers for removing them from the caches.

However, if the attacker wants to generate the forge digital signature \(S^* = (\Omega_pW + d)\) and launching the content poisoning attack, then it needs to calculate a random private
number $d$ from $\mathcal{L} = \{d, \mathcal{D}\}$ and private key of the provider $\mathcal{P}$ from $\mathcal{W} = \{\mathcal{P}, \mathcal{D}\}$. Here, finding $d$ and $\mathcal{P}$ are the two discrete logarithm problems over the Hyperelliptic curve and therefore infeasible to break two-time discrete logarithm problems.

So, from the aforementioned discussions, we can say that our scheme is safe against the Attacker to launch a content poisoning attack.

V. DISCUSSION AND COMPARISONS
In this section, we compared our scheme with two different types of schemes, i.e. i) NDN-based schemes for content poisoning attack prevention and ii) identity-based signature schemes.

A. NDN-BASED SCHEMES
The existing NDN-based schemes for mitigation of content poisoning attack don’t have any proper signature verification mechanism. So, we compare our scheme with [13], [15], [21], [22], and [24] on the basis of latency, verification overhead, and security as shown in Table 2. In Addition, we also explain the reason for their weaknesses in the respective schemes.

Ghali et al. [13], the ranking algorithm scheme differentiate between valid and fake content objects based on observed consumer’s behavior. The scheme verifies and provides ranking to every content according to consumer’s feedback. The scheme works with low latency and eliminates the extra overhead problem due to verifying only cache hit contents according to the client’s feedback. However, the security of the scheme is weak, because it is totally depended on client feedback. Any attacker can give positive feedback about the invalid provider and malicious router or negative feedback about a valid provider and router. The illegal users can interest for a number of non-popular contents, so NDN routers attach provider key and store the return contents copies in every intermediate router CS between clients and providers. Our scheme reduces the verification overhead. Further, our scheme is strongly secured and stops other attacks because it ensures the security properties of authenticity, integrity, unforgeability, and non-repudiations.

Kim et al. [15] divide the contents into two types; cache hit and cache miss. In case of the cache hits it stores the contents otherwise bypassed it. The scheme works with high latency and extra verification overhead, due to the verification process that occurs for every chunk that is requested twice. Further, the security level of the scheme is an average due to verifying cache hit contents twice. However, in the proposed scheme, any attacker can verify and store non-popular and invalid contents and further request for it many times. As compared to this scheme our proposed scheme works on low latency and very less verification overhead due to the identity-based signature verification process because it removes the certificate management issues. In addition, our scheme provides protection from cache pollution attacks because it broadcast the invalid contents and hence eliminates the invalid content from CS of the router.

Wu et al. [21] proposed ROM, the Router-Oriented Mitigation to temporarily remove the injected routers from the transmission. A router can be considered injected if they show any abnormal behavior or client give negative feedback about it. The scheme is suffering from high latency due to removing router in on-path transmission and divergence of path. Further, by putting all traffic on one side can create extra overhead. If there is no alternative path for the transmutation, then what to do. As compared to this scheme our scheme works with low latency and produces high security due to on-demand verification.

Mai et al. [22] scheme that passes every content from NDN firewall and micro detectors in Bayesian Network techniques to mitigate content poison attack. The authors connect alarm with micro detectors that activate when any significant changes occur from its normal to abnormal behavior of nodes. The scheme works with high latency and extra overhead due to passing every content from firewall and micro detectors. The proposed scheme passes every popular and non-popular content from the micro detector. On the other hand, our scheme solves the latency problem due to the identity-based signature verification process. Further, our scheme provides strong security by offering the security properties of authenticity, integrity, unforgeability, and non-repudiations that stop content poisoning attack as compared to Mai et al. [22] scheme.

Hu et al. [24] proposed a light-weight mitigation mechanism name key-based forwarding and multipath forwarding-based inband prob. Before forwarding every interest, the router should attach the public key of the provider from FIB to interest. If any on-path poisoning content/router found the inband will change the path from the poisoning content/router. The scheme facing latency problems due to the changing path during transmission. Also, interest can be forwarded towards where is no source available for data. Hu et al. [24] scheme is not suitable for large and complex networks due to attaching provider public key with every interest. If there is no public key of the specific content provider in FIB that the client wants then what will be done, no solution given by the authors. Our proposed scheme works with minimum latency and strong security without the need for provider public key with interest. Further, our scheme stops content poisoning attack with a broadcast that eliminates poison content from the cache.

B. IDENTITY-BASED SCHEMES
In this section, we compare our schemes with the existing schemes on the basis of computation and communication costs.

1) COMPUTATION COST
In this section, the comparison in terms of computation cost is made between the proposed and those of Sharma et al. [51], James et al. [52], Sharma and Sharma [34].
**TABLE 3.** Computational cost comparison in terms of major operations.

| Schemes                  | Signer | Verifier | Total   |
|--------------------------|--------|----------|---------|
| G. Sharma et al. [51]    | 2 $\Sigma$PM | 1 $\Sigma$PM | 3 $\Sigma$PM |
| James et al. [52]        | 1 $\Sigma$PM | 2 $\Sigma$PM | 3 $\Sigma$PM |
| N. Sharma and B. K.      | 1 $\Sigma$PM | 1 $\Sigma$PM | 2 $\Sigma$PM |
| Sharma [34]              | 5 $\Sigma$PM | 4 $\Sigma$PM | 9 $\Sigma$PM |
| Krishna et al. [53]      | 2 $\Sigma$PM | 1 $\Sigma$PM | 3 $\Sigma$PM |
| R. Yaduvanshi and S. Mishra [35] | 2 $\Sigma$PM | 1 $\Sigma$PM | 3 $\Sigma$PM |
| Proposed scheme          | 2 $\Sigma$CDM | 2 $\Sigma$CDM | 4 $\Sigma$CDM |

**TABLE 4.** Time comparison of computation cost in milliseconds.

| Schemes                  | Signer | Verifier | Total   |
|--------------------------|--------|----------|---------|
| G. Sharma et al. [51]    | 1.94   | 0.97     | 2.91    |
| James et al. [52]        | 14.90  | 29.8     | 44.7    |
| N. Sharma and B. K.      | 14.90  | 14.90    | 29.8    |
| Sharma [34]              | 4.85   | 3.88     | 8.73    |
| Krishna et al. [53]      | 1.94   | 0.97     | 2.91    |
| R. Yaduvanshi and S. Mishra [35] | 0.97 | 0.97 | 1.97 |
| Proposed scheme          | 0.97   | 0.97     | 1.97    |

Krishna et al. [53], and Yaduvanshi and Mishra [35]. The comparison includes the expansive mathematical operations, which is used in the proposed and in the aforementioned existing schemes such as bilinear pairing operation ($B\hat{P}$), elliptic curve point multiplication ($\Sigma$PM), and Hyperelliptic curve divisor multiplication ($\hat{h}\Sigma$CDM). Here, the minor operation like addition, division, subtraction, encryption, decryption, and hash that require less time during computation being ignored. We showed the required major operation in Table 3 for Sharma et al. [51], James et al. [52], Sharma and Sharma [34], Krishna et al. [53], Yaduvanshi and Mishra [35], and for our proposed scheme, respectively. Additionally, in Table 4, we provide a comparison by utilizing these major operations with respect to milliseconds (ms). By assuming the experiments produced in [61] with the following mentioned system specification.

- Intel Core i7 4510UCPU
- 2.0 GHz with 8 GB RAM
- Windows 7
- Multi-precision Integer and Rational Arithmetic C Library (MIRACL).

According to [61], $B\hat{P}$ will consume 14.90ms, $\Sigma$PM will consume 0.97ms. Supposing the same system environment provided in [61] $\hat{h}\Sigma$CDM will take 0.48ms respectively [58], [62].

**Computation Cost Reduction of the Proposed Scheme From the Existing Schemes:**

Cost reduction can be calculated by using the following formula.

$$\left(\frac{\text{existing scheme} - \text{proposed scheme}}{\text{existing scheme}}\right) \times 100$$

- Reduction of the proposed scheme from Sharma et al. [51] as:

$$\left(\frac{3 \Sigma\text{PM} - 4\hat{h}\Sigma\text{CDM}}{3 \Sigma\text{PM}}\right) \times 100$$

$$= \left(\frac{2.91 - 1.97}{2.91}\right) \times 100 = 32.30\%$$

- Reduction of the proposed scheme from James et al. [52] as:

$$\left(\frac{3 \Sigma\text{PM} - 4\hat{h}\Sigma\text{CDM}}{3 \Sigma\text{PM}}\right) \times 100$$

$$= \left(\frac{44.7 - 1.97}{44.7}\right) \times 100 = 95.59\%$$

- Reduction of the proposed scheme from Sharma and Sharma [34] as:

$$\left(\frac{2 B\hat{P} - 4\hat{h}\Sigma\text{CDM}}{2 B\hat{P}}\right) \times 100$$

$$= \left(\frac{29.8 - 1.97}{29.8}\right) \times 100 = 97.31\%$$

- Reduction of the proposed scheme from Krishna et al. [53] as:

$$\left(\frac{9 \Sigma\text{PM} - 4\hat{h}\Sigma\text{CDM}}{9 \Sigma\text{PM}}\right) \times 100$$

$$= \left(\frac{8.73 - 1.97}{8.73}\right) \times 100 = 77.43\%$$

- Reduction of the proposed scheme from Yaduvanshi and Mishra [35] as:

$$\left(\frac{3 \Sigma\text{PM} - 4\hat{h}\Sigma\text{CDM}}{3 \Sigma\text{PM}}\right) \times 100$$

$$= \left(\frac{2.91 - 1.97}{2.91}\right) \times 100 = 32.30\%$$

In Figure 6, we have shown the computational cost reduction.

**C. COMMUNICATION OVERHEAD**

In this section, we compared our proposed scheme with the existing schemes i.e., Sharma et al. [51], James et al. [52], Sharma and Sharma [34], Krishna et al. [53], and Yaduvanshi and Mishra [35] with respect to communication overhead. For this purpose, we assume $|l| = 160$ bits for elliptic curve, $|l| = 1024$ bits for bilinear pairing, $|ID| = 160$ bits, $|l| = 80$ bits for a Hyperelliptic curve, and $|ID| = 100$ bits for message respectively. According to our supposition the communication cost for Sharma et al. [51] scheme is $|l| + |ID| + 3|l|$, for James et al. [52] scheme is $2|l|$, for Sharma and Sharma [34] is $|l| + 3|l|$, for Krishna et al. [53] is $|l| + 3|l|$, and for Yaduvanshi and Mishra [35] is $2|l|$, and for our proposed scheme is $|l| + 3|l|$ respectively. Thus, it is clear from the Table 5,
the proposed scheme is better in communications cost than Sharma et al. [51], James et al. [52], Sharma and Sharma [34], Krishna et al. [53], and Yaduvanshi and Mishra [35]. Further, in Figure 7, a communication overhead cost reduction is shown.

**Communication Overhead Reduction of the Proposed Scheme From the Existing Schemes in Terms of Bits:**

Cost reduction can be calculated by using the following formula.

\[
\left( \frac{\text{existing scheme} - \text{proposed scheme}}{\text{existing scheme}} \right) \times 100
\]

- **Reduction of the proposed scheme from Sharma et al. [51] as:**

\[
\left( \frac{11n + 1\mid ID + 3\mid q - 11n + 3\mid q}{11n + 1\mid ID + 3\mid q} \right) \times 100
\]

\[
= \left( \frac{1100 + 160 + 3160 - 1100 + 3180}{1100 + 160 + 3160} \right) \times 100
\]

\[
= \left( \frac{760 \text{ bits} - 340 \text{ bits}}{760 \text{ bits}} \right) \times 100 = 55.26\%
\]

- **Reduction of the proposed scheme from James et al. [52] as:**

\[
\left( \frac{11n + 2\mid I + 3\mid q - 11n + 3\mid q}{11n + 2\mid I + 3\mid q} \right) \times 100
\]

\[
= \left( \frac{1000 + 21024 + 31024 - 1000 + 3180}{1000 + 21024} \right) \times 100
\]

\[
= \left( \frac{2148 \text{ bits} - 340 \text{ bits}}{2148 \text{ bits}} \right) \times 100 = 84.17\%
\]

- **Reduction of the proposed scheme from Sharma and Sharma [34] as:**

\[
\left( \frac{11n + 3\mid I + 2\mid I - 11n + 3\mid I}{11n + 3\mid I} \right) \times 100
\]

\[
= \left( \frac{1000 + 31024 - 1000 + 3180}{1000 + 31024} \right) \times 100
\]

\[
= \left( \frac{3172 \text{ bits} - 340 \text{ bits}}{3172 \text{ bits}} \right) \times 100 = 89.28\%
\]
• Reduction of the proposed scheme from Krishna et al. [53] as:
  \[
  \left( \frac{1|n| + 3|q| - |n| + 3|p|}{|n| + 3|q|} \right) \times 100
  = \left( \frac{|100| + 3|160| - |100| + 3|80|}{|100| + 3|160|} \right) \times 100
  = \left( \frac{580 \text{ bits} - 340 \text{ bits}}{580 \text{ bits}} \right) \times 100 = 41.37 \%
  \]

• Reduction of the proposed scheme from Yaduvanshi and Mishra [35] as:
  \[
  \left( \frac{1|n| + 2|q| - |n| + 3|p|}{|n| + 2|q|} \right) \times 100
  = \left( \frac{|100| + 2|160| - |100| + 3|80|}{|100| + 2|160|} \right) \times 100
  = \left( \frac{420 \text{ bits} - 340 \text{ bits}}{420 \text{ bits}} \right) \times 100 = 19.04 \%
  \]

VI. APPLICATION SCENARIO OF THE PROPOSED SCHEME

In this section, we consider the NDN-based smart city network, where a number of sensors and routers are deployed to produce different contents as shown in Figure 8. Moreover, the things in the smart city are connected based on the NDN policy. During communication and transmission in the NDN-based smart city, the forwarding is based on name-based routing with in-network content caching. In NDN-based smart city every node maintains three types of data structures, namely Content Store (CS), stores the copy of the contents with itself in the CS for future use, Pending Interest Table (PIT), the PIT stores all the interests that a router has forwarded but not satisfied yet, and Forwarding Information Base (FIB), used to forward the requests from one router to another based on routing protocols [24].

Suppose two smart things want to communicate with each other, here the communication will consist of three participants, namely; client, network manager, and provider.

The client is those who require content, the provider is those who provide content to the client, and the network manager is a fully trusted third party, who is responsible for secure communication among the client and the provider as further shown in Figure 9.

The secure communication between client and provider is mentioned in the following phases;

1. **Registration Phase**: In this phase, the client and the provider need to register themselves with the network manager by sending their Identities \(3d_u\). The network manager gets their Identities \(3d_u\) and generate a private key \(\Omega_u = (v_u + \zeta.N) \mod q\) and public key \(w_u = v_u.D\), for the user by using their identity \(3d_u\). Then the network manager sends the \(\Omega_u\) and \(w_u\) to both client and provider.

2. **Signature Generation Phase**: when the client shows an interest in content \(C\), after receiving the interest the provider will digitally sign \(C\). For this purpose, the provider takes the Divisor D, the private key of the provider \(\Omega_p\) and the content \(C\) as an input to produce a sign tuple \(\delta = (\mathcal{E}, W, L, S)\). For signing the tuple \(\delta\)
the provider first Randomly chooses \( d \in \{1, 2, 3, \ldots, q - 1\} \) and Computes \( \mathcal{L} = d \cdot D \mod q \) where \( D \) is the divisor of the Hyperelliptic curve. Then after, the provider computes content digest \( W = h_1(C//L//N_r) \), set \( W = MD_2 \), and \( N_r \) is the fresh nonce.

Further, the digital signature \( S = (\Omega_w W + d) \mod q \) and finally generated a signed tuple \( \delta = (C, W, L, S) \) and send it to the client.
Verification Phase: After receiving the signed tuple
\( \delta = (\mathcal{C}, \mathcal{W}, \mathcal{L}, \mathcal{S}) \), the client can verify the contents in the following steps: It computes content digests
\( \mathcal{W} = h_1(\mathcal{C} // \mathcal{L} // \mathcal{N} // 3d_p) \), set \( \mathcal{W} = MD_2 \), computes
\( \delta.D = \mathcal{W} (w_p + \beta) + \mathcal{L} \) for signature verification, and compare \( MD_2 = MD_1 \) for integrity, if it is not holds, then it means that the content is poisoned.

3. Poisoned Content Removing: Once the content is poisoned, then the client encrypts the poisoned contents and \( MD_2 \) as \( OJ = \varepsilon wp(C, MD_2) \), sends \( POJ \) to the original provider. So, after receiving \( POJ \), the publisher decrypts \( (AMD_2) = Dwp(POJ) \), compares \( MD_2 \) with its valid content \( MD_1 \) as \( MD_2 = MD_1 \). If the equality does not hold, then the original provider broadcasts a message regarding this poisoned content in the networks to remove it from the router caches.

VII. CONCLUSION
In this paper, we proposed an efficient and formally secure identity-based signature scheme for preventing content poisoning attack in IoT-based NDN networks. First, the proposed scheme is compared with NDN-based security schemes with respect to the content poisoning attack and the results show that our scheme provides strong security with low latency against content poisoning attack. Then, the newly designed scheme is compared with the existing identity-based signature schemes in terms of computational cost and communication overhead. The proposed scheme reduces the computational cost from 32.30% to 97.31% and communication overhead from 19.04% to 89.28% from the existing schemes. In addition, we validate the security requirement of the proposed scheme through AVISPA formally and the Simulation results show that our scheme is SAFE under the two back end protocol i.e. ATSE and OFMC. Moreover, the contributed scheme provided a provable security under the random oracle model (ROML) regarding existential unforgeability against adaptive chosen content (message) attack (EUF – IBS – ACCA). To conclude, we provided a practical application scenario of the proposed scheme on the NDN-based smart city network.

APPENDIX
In this section, we discuss and validate the proposed scheme with the well-known simulation tool AVISPA. The code and results are shown in the following subsection

A. VALIDATION OF INTERNET SECURITY PROTOCOLS AND APPLICATIONS (AVISPA)
For the simulation, we use the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. AVISPA is an automatic tool that proves the validation of cryptographic schemes in terms of SAFE or UNSAFE mode. According to the HLPSL language syntax and rules, AVISPA provides results of the development scheme. The code is written using the rules of HLPSL. The intermediate format (IF) converts written code into lower-level machine language.

![Figure 10. Top down flow of AVISPA.](image)

Translation to IF is achieved with the help of HLPSL to the IF translator. Clark and Jacob [59], [60] suggest that HLPSL2IF translator orders the execution of the judgment by given primary knowledge, every agent can build the messages he/she imagines.

AVISPA tool uses On-the-fly Model-Checker (OFMC), CL-based Attack Searcher (CLAtSe), SAT-based Model-Checker (SATMC), and Tree-Automata-based Protocol Analyzer (TA4SP), the back end for their work as shown in Figure 10. As required, every back end provides its own functionality.

B. PROVIDER ROLE
In this part, we explain the provider role. In our scheme, the provider digitally signs the content with its private key for the signature generation and hash value. The HLPSL code for the provider role is shown in Table 6.

### TABLE 6. Provider role HLPSL code.

| role role_Podr(Podr:agent,Cntv:agent,Yp:public_ |
| key,SND,RCV:channel(dy)) |
| played_by Podr |
| def= |
| local |
| State=nat,As:text,R:text,W:text,D:text |
| init |
| State := 0 |
| transition |
| 1. State=0 \& RCV(start) \implies State'=1 \& SND(Podr,Cntv) |
| 2. State=1 \& RCV(Cntv,\{As\} \_Yp) \implies State'=2 \& D'=\_new() \& R'=\_new() \& W'=\_new() \& SND(Podr,\{W:\_R:\_D\} \_inv(Yp)) |
| end role |
FIGURE 11. Result of proposed scheme on the base of OFMC protocol.

TABLE 7. Client role HLPSL code.

| Role             | Code                                                                 |
|------------------|----------------------------------------------------------------------|
| role role_Cntv(Podr:agent,Cntv:agent,Yp:public_key,SND,RCV:channel(dy)) | def=                                                               |
|                  | local                                                                |
|                  | State:nat,As:text,R:text,W:text,D:text                               |
|                  | init                                                                 |
|                  | State := 0                                                           |
|                  | transition                                                           |
|                  | 1. State=0 ∧ RCV(Podr,Cntv) =⇒ State':=1 ∧ As':=new() ∧ SND(Cntv, {As'}_Yp) |
|                  | 6. State=1 ∧ RCV(Podr, {W',R',D'}_inv(Yp)) =⇒ State':=2             |
|                  | end role end role                                                    |

C. CLIENT ROLE

In this subsection, we explain the role of the client in our proposed scheme. If the client wants verification of content and provider, they need to get the public key of the provider. With the provider public key, the client can check authenticity of the provider. The client role HLPSL code is shown in Table 7.

D. PROVIDER VERIFICATION AND BROADCAST

This subsection combines the role of client-side verification and broadcasting invalid content to remove it from CS. A client can verify the provider with public key. In case of invalidity, the client send the poison content to the network manager. Network manager, broadcasts the poison content networks for removing this poisoned content from different CS’s of nodes. The HLPSL code for provider verification and broadcasting is shown in Table 8.

E. SIMULATION RESULT OF PROPOSED SCHEME

In this section, we present the simulation results according to the above-stated HLPSL code. We apply HLPSL code on following two protocols.
FIGURE 12. Results of proposed scheme on the base of ATSE protocol.

1) OFMC PROTOCOL RESULT
The HLPSL code for the OFMC protocol shows that our scheme is SAFE as it prevents the IoT-based NDN from content poisoning attack. The results are shown in Figure 11.

2) ATSE PROTOCOL RESULT
The HLPSL code for the ATSE protocol shows the safety of our proposed scheme. This scheme is efficient to prevent IoT-based NDN from content poisoning attack. The results of this protocol are shown in Figure 12.

REFERENCES
[1] L. Patrono, L. Atzori, P. Šolić, M. Mongiello, and A. Almeida, “Challenges to be addressed to realize Internet of Things solutions for smart environments,” Future Gener. Comput. Syst., Sep. 2019, doi: 10.1016/j.future.2019.09.033.
[2] R. Boussada, B. Hamdane, M. E. Elhdhili, and L. A. Saidane, “PP-NDNoT: On preserving privacy in IoT-based E-health systems over NDN,” in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2019, pp. 1–6, doi: 10.1109/WCNC.2019.8886110.
[3] V. Jacobson, J. Burke, D. Estrin, L. Zhang, B. Zhang, G. Tsudik, K. Claffy, D. Krioukov, D. Massey, C. Papadopoulos, and P. Ohm, “Named data networking (NDN) project principal investigators,” Dept. Comput. Sci., Long Beach, CA, USA, Tech. Rep., 2013.
[4] K. Ahed, M. Benamar, and R. El Ouazzani, “Content delivery in named data networking based Internet of Things,” in Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC), Jun. 2019, pp. 1397–1402, doi: 10.1109/IWCMC.2019.8766526.
[5] B. Nour, H. Ibne-Khedher, H. Moungla, H. Afifi, F. Li, K. Sharif, H. Khelifi, and M. Guizani, “Internet of Things mobility over information-centric/named-data networking,” IEEE Internet Comput., vol. 24, no. 1, pp. 14–24, Jan. 2020, doi: 10.1109/MIC.2019.2963187.
[6] M. Amadeo, G. Ruggeri, C. Campolo, and A. Molinaro, “IoT services allocation at the edge via named data networking: From optimal bounds to practical design,” IEEE Trans. Netw. Service Manage., vol. 16, no. 2, pp. 661–674, Jun. 2019, doi: 10.1109/TNSM.2019.2900274.
A. Detti, A. Caponi, G. Tropea, G. Bianchi, and N. Blefari-Melazzi, “On the interplay among naming, content validity and caching in information centric networks,” in Proc. IEEE Global Commun. Conf. (GLOBECOM), Dec. 2013, pp. 2108–2113, doi: 10.1109/GLOCOM.2013.6831386.

S. DiBenedetto and C. Papadopoulos, “Mitigating poisoned content with forwarding strategy,” in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Apr. 2016, pp. 164–169, doi: 10.1109/INFOCOM.2016.7562065.

D. Wu, Z. Xu, B. Chen, and Y. Zhang, “What if routers are malicious? Mitigating content poisoning attack in NDN,” in Proc. 15th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun., 10th IEEE Int. Conf. Big Data Sci. Eng., 14th IEEE Int. Symp. Parallel Distr. Process. Appl., Aug. 2016, pp. 481–488, doi: 10.1109/TrustCom.2016.0100.

H. L. Mai, T. Nguyen, G. Doyen, R. Cogranne, W. Mallouli, E. M. de Oca, and O. Fester, “Towards a security monitoring plane for named data networking and its application against content poisoning attack,” in Proc. IEEE/IFIP Netw. Operations Manage. Symp. (NOMS), Apr. 2018, pp. 1–9, doi: 10.1109/NOMS.2018.8406240.

H. L. Mai, M. Aoudai, G. Doyen, D. Kondo, X. Marchal, T. Cholez, E. M. de Oca, and W. Mallouli, “Implementation of content poisoning attack detection and reaction in virtualized NDN networks,” in Proc. 21st Conf. Innov. Clouds, Internet Netw. Workshops (ICIN), Feb. 2018, pp. 1–3, doi: 10.1109/ICIN.2018.8401591.

X. Hu, J. Gong, G. Cheng, G. Zhang, and C. Fan, “Mitigating content poisoning with name-key based forwarding and multipath forwarding based inband probe for energy management in smart cities,” IEEE Access, vol. 6, pp. 39692–39704, 2018, doi: 10.1109/ACCESS.2018.2854928.

R. Perfman, “An overview of PKI trust models,” IEEE Netw., vol. 13, no. 6, pp. 38–43, Nov./Dec. 1999, doi: 10.1109/65.806987.

X. Yang, X. Pei, G. Chen, T. Li, M. Wang, and C. Wang, “A strongly unforgeable certificatesless signature scheme and its application in IoT environments,” Sensors, vol. 19, no. 12, p. 2692, Jun. 2019, doi: 10.3390/s19122692.

A. Shamir, “Identity-based cryptosystems and signature schemes,” in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science: Lecture Notes Artificial Intelligence: Lecture Notes Biometrics), pp. 196. 1995, pp. 47–53, doi: 10.1007/3-540-59658-7_5.

D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” in Advances in Cryptology—ASIACRYPT, vol. 2248, 2001, pp. 514–532.

D. Boneh, M. Franklin, “Identity-based encryption from the Weil pairing,” SIAM J. Comput., vol. 23, no. 3, pp. 586–615, 2003.

D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” SIAM J. Comput., vol. 22, no. 2, pp. 213–229, 1993.

R. A. Sahu and S. Padhye, “Identity-based digital signature scheme without forward security,” in Proc. Int. Conf. Trust. Secur. Priv. Comput. Commun., 10th IEEE Int. Conf. Big Data Sci. Eng., 14th IEEE Int. Symp. Parallel Distr. Process. Appl., Aug. 2016, pp. 481–488, doi: 10.1109/TrustCom.2016.0100.

H. L. Mai, T. Nguyen, G. Doyen, R. Cogranne, W. Mallouli, E. M. de Oca, and O. Fester, “Towards a security monitoring plane for named data networking and its application against content poisoning attack,” in Proc. IEEE/IFIP Netw. Operations Manage. Symp. (NOMS), Apr. 2018, pp. 1–9, doi: 10.1109/NOMS.2018.8406240.

S. Ullah et al.: Lightweight IBS Scheme for Mitigation of Content Poisoning Attack in NDN With IoT

H. Du and Q. Wen, “An efficient identity-based short signature scheme from bilinear pairings,” in Proc. Int. Conf. Comput. Intell. Secur., Dec. 2007, pp. 725–729, doi: 10.1109/CISC.2007.168.

R. T. Okamoto and E. Okamoto, “Efficient short signature from pairing,” in Proc. 5th Int. Conf. Inf. Technol. New Generat., 2009, pp. 417–422, doi: 10.1109/ITNG.2009.176.

L. Zhang, Y. Hu, and Q. Wu, Short Signature From The Bilinear Pairing (Lecture Notes in Computer Science: Lecture Notes Artificial Intelligence: Lecture Notes Biometrics), vol. 6377. Berlin, Germany: Springer, 2010, pp. 111–118, doi: 10.1007/978-3-642-16167-4_1015.

S. Mishra, R. A. Sahu, S. Padhye, and R. S. Yadav, “Efficient ID-based multi-proxy signature scheme from bilinear pairing based on K-plus problem,” Commun. Comput. Inf. Sci., vol. 165, pp. 113–122, 2011, doi: 10.1007/978-3-642-22247-4_10.

D. He, J. Chen, and J. Hu, “Identity-based digital signature scheme without bilinear pairings,” IACR Cryptol. ePrint Arch., vol. 79, Feb. 2011.

N. Sharma and B. K. Sharma, “Identity-based signature scheme using random oracle model,” J. Comput. Math. Sci., vol. 9, no. 4, pp. 254–263, Apr. 2018, doi: 10.29059/j cms/754.

R. Yaduvanshi and S. Mishra, “An efficient and secure pairing free short ID-based signature scheme for elliptic curve,” in Proc. 2nd Int. Conf. Adv. Comput. Softw. Eng. (ICACSE), Sultnagar, India: Department of Computer Science and Engineering, Kamla Nehru Institute of Technology, Feb. 2019, pp. 5.

A. Fiat and A. Shamir, “How to prove yourself: Practical solutions to identification and signature problems,” in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science: Lecture Notes Artificial Intelligence: Lecture Notes Biometrics), pp. 263. 1987, pp. 186–194, doi: 10.1007/3-540-47721-7_12.

R. A. Sahu and S. Padhye, “ID-based signature schemes from bilinear pairing: A survey,” Frontiers Electr. Electron. Eng. China, vol. 6, no. 4, pp. 487–500, Dec. 2011, doi: 10.1007/s11460-011-0119-1.
[60] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, and L. Compagna, “The AIVSPA tool for the automated validation of Internet security protocols and applications,” in Computer Aided Verification, vol. 3576, 2005, pp. 281–285.

[61] C. Zhou, Z. Zhao, W. Zhou, and Y. Mei, “Certificateless key-insulated general- ized signcryption scheme without bilinear pairings,” Secur. Commun. Netw., vol. 2017, pp. 1–17, Aug. 2017.

[62] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi, F. U. Khanzada, and N. U. Amin, “An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network,” IEEE Access, vol. 8, pp. 36807–36828, 2020.

SYED SAJID ULLAH received the master’s degree in computer science from Hazara University Mansehra, Pakistan, in 2017, where he is currently pursuing the M.S. degree. His major research domains are cryptography, network security, information centric networking (ICN), named data networking (NDN), and the IoT.

INSAF ULLAH received the M.S. degree in computer sciences from the Department of Information Technology, Hazara University Mansehra, Pakistan, where he is currently pursuing the Ph.D. degree in computer sciences. He is also serving as a Lecturer with the Department of Computer Sciences, Hamdard University, Islamabad. His research interests include network security, UAVs/Drones, information centric networking (ICN), named data networking (NDN), the IoT, the IoT, wireless sensor networks (WSN), wireless body area networks (WBAN), and cryptography.

HIZBULLAH KHATTAK received the Ph.D. degree from Hazara University Mansehra, Pakistan, in 2018. His major research domains are information-centric networking, networks security, mobile adhoc networks, and the Internet of Things (IoT).

MUHAMMAD ASGHAR KHAN received the bachelor’s degree in electronic engineering from Iqra University, Karachi, Pakistan, and the master’s degree in electrical engineering from the Center of Advanced Studies in Engineering (CASE), Islamabad, Pakistan. He is currently pursuing the Ph.D. degree in electronic engineering with the School of Engineering and Applied Sciences (SEAS), ISRA University, Islamabad. He is also serving as a Lecturer with the Department of Electrical Engineering, Hamdard University, Islamabad. His research interests include UAVs/Drones and the IoT with a focus on networks, platforms, security, as well as applications and services. He is a reviewer of various journals published by the IEEE, Elsevier, MDPI, and EURASIP.

MUHAMMAD ADNAN received the B.S. degree from the University of Peshawar, Peshawar, Pakistan, in 2006, the M.S. degree from the Center for Advanced Studies in Engineering, Islamabad, Pakistan, in 2008, and the Ph.D. degree from Dongguk University, Seoul, South Korea, in 2016. He worked as a Lecturer in different public sector universities of Pakistan, from 2008 to 2012, and 2016 to 2018. He has done his Postdoctoral Researcher from the College of Information Technology, United Arab Emirates (UAE) University, UAE. He is currently a Faculty Member with the Higher Colleges of Technology, Al Ain Men’s College, UAE. His research interests include wireless networks, resource management, energy efficiency, and the IoT for health care.

SADAM HUSSAIN received the bachelor’s degree from Islamia College University, Peshawar, Pakistan, in 2017. He is currently pursuing the M.S. degree with Hazara University Mansehra, Pakistan. His major research domains are cryptography, network security, wireless sensor networking (WSN), information centric networking (ICN), named data networking (NDN), smart grids, the Internet of Things (IoT), the IoT, cloud computing, and edge computing.

NOOR UL AMIN received the master’s degree in computer science from the University of Peshawar, Pakistan, in 1996, and the Ph.D. degree in computer science from the Department of Information Technology, Hazara University, Pakistan. He was the Head of the Department of Information Technology and the Director of IT, Hazara University, for 11 years, where he is currently the Chair of the Department of Telecommunication. He has completed recently a Research and Development project sponsored by the Ministry of Science and Technology, Pakistan. He has established seven hi-tech research and development labs.

MUAZZAM A. KHAN KHATTAK (Senior Member, IEEE) received the Ph.D. degree in computer sciences as a sandwich program from IIUI and UMKC, USA, in 2011. He received his Postdoctoral Researcher from the University of Missouri, Kansas City, MO, USA, in 2016. He joined the School of Electrical Engineering and Computer Science (ECECS), NUST University, Islamabad, as an Assistant Professor, in 2013, and later on promoted to the Associate Dean and a Tenured Associate Professor, in 2017. He has been with the School of Computer Science, University of Ulm, Germany, and the School of Computer and the Electrical Engineering, University of Missouri, as a Research Fellow. He worked at the Networking and Multimedia Laboratory, University of Missouri Kansas City, USA, as a Research Fellow. He is currently working as a Tenured Associate Professor with the Department of Computer Science, Quaid-i-Azam University, Islamabad, Pakistan. His research interests include wireless networks sensor, body area networks, image processing, image compression, image encryption, and data network security.

* * *